CITY OF OAKLAND

Privacy Advisory Commission

July 2, 2020 4:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Agenda

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

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

Pursuant to the Governor's Executive Order N-29-20, members of the Privacy Advisory Commission, as well as City staff, will participate via phone/video conference, and no physical teleconference locations are required.

Please click the link below to join the webinar:
https://us02web.zoom.us/j/89905819645

Or iPhone one-tap :

US: +16699009128, 89905819645# or +13462487799,,89905819645#

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 or +1 301 715 8592 or +1 312 626 6799

Webinar ID: 899 0581 9645

International numbers available: https://us02web.zoom.us/u/kdnHuPhWBb

1. Call to Order, determination of quorum

2. Open Forum/Public Comment

3. Review and approval of the draft June meeting minutes

4. Goldman School of Public Policy – Oakland Resident Data report – review and take possible action.

5. Federal Task Force Transparency Ordinance – OPD – FBI's Joint Terrorism Task Force 2019 Annual Report – review and take possible action.

6. Commission Workplan Revision – Chair – review.

7. Surveillance Equipment Ordinance Amendments – Hofer/Patterson – review and take possible action.

    a. Prohibition On Predictive Policing Technology
    b. Prohibition on Biometric Surveillance Technology
    c. Annual Report metrics and due date

8. Surveillance Equipment Ordinance – OPD – Forensic Logic Impact Report and proposed Use Policy - review and take possible action.

CITY OF OAKLAND

Privacy Advisory Commission

June 4, 2020 4:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Minutes

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

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum

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

2. Open Forum/Public Comment

Assada Olugbala spoke about her concern that the PAC has regulatory power over OPD outside the scope of the Police Commission. She referenced the ordinance that requires Law Enforcement MOUs to first come before the PAC as an example of something she feels belongs in the Police Commission Purview.

3. Review and approval of the draft May meeting minutes

The May Minutes were approved unanimously.

4. Federal Task Force Transparency Ordinance – OPD – FBI's Joint Terrorism Task Force 2019 Annual Report – review and take possible action.

The Chair first called for Public Speakers and 5 spoke to the item:

Jeffrey Wang asked that the OPD, upon approval from the PAC, ensure they also report out to the Public Safety Committee and City Council as required in the ordinance.
Javeria Jamil commented that JTTFs around the country have recently been used to monitor protests in the wake of the George Floyd killing and to investigate Antifa and Black Lives Matter organizers making the need to monitor what activities OPD engages in with them critical.
Mohamed Talib echoed Javeria's comments and argued that OPD should withdraw from the JTTF altogether.
Husam Falah also urged OPD to send the report to the City Council for consideration. He noted that he has seen members of his community targeted and with OPD's history in consideration, transparency is important.
Asada Olugbala drew a comparison between this reporting requirement that is relatively new and the Negotiated Settlement that OPD has been under for 17 years. She feels the older settlement is a far higher priority for OPD to complete.

The Chair asked why OPD lists a homicide case in the report and Sgt. Daza-Quiroz explained it was a tip that originated from a JTTF effort that was provided to OPD. Chair Hofer also asked why a "duty to inform" was not listed and the Sgt. explained that since the FBI already reported it, OPD did not need to.

Member Suleiman asked about the three cases listed but not discussed in the report and noted that in Portland, the JTTF report provides a higher level of detail including demographic details. Sgt. Daza-Quiroz said he could look at the Portland Report and see what else he could add to Oakland's.

Chair Hofer asked about why the 2018 report had not yet gone to Council and Brice Stoffmacher explained he wanted to coordinate the report to go to Council along with the MOU.

There was discussion about the City Council Schedule and whether there would be a Public Safety Committee to send the report to or whether it would go to the full Council. Sgt. Daza-Quiroz agreed to see what additional info he could get to include in the report and the item was tabled until the next meeting.

5. Surveillance Equipment Ordinance – OPD – Forensic Logic Impact Report and proposed Use Policy - review and take possible action.

Chairperson Hofer offered for OPD to provide any opening thoughts and Captain Bassett spoke about the progress on the policy thus far including a demonstration meeting with some PAC Members to better understand the use.

The PAC reviewed the updated documents and had several questions about what was included and how Forensic Logic tools are used by OPD. Chair Hofer listed a couple of areas of concern that would need to be resolved before supporting moving forward:

Predictive policing—the Impact Statement states that no Predictive Policing is used but in the FL Manual, "Next Crime" is described as a predictive policing. Understanding and defining Predictive Policing was discussed at length.

Additionally, the Chair raised concerns about third party data sharing and other components that FL has available to the City. Another example is the FL "Tips and Alerts" function and whether that data is integrated into the technology and accessible.

Member Suleiman had similar questions about outside databases and third party data sharing; hoping to see more information about what other data may be fed into the system from elsewhere (including law enforcement and non-law enforcement sources.

Robert Batty with Forensic Logic provided a lot of feedback and answers to many of the questions of the PAC.

Member Oliver raised concerns about the concept of predictive policing and the fact that using past data where OPD is heavily deployed, becomes a self-fulfilled prophesy directing more resources to those neighborhoods which can create a disparate impact. He also has concerns that OPD will want to share their data they collect with other agencies (which may not have the same restrictions on how the data is used).

Member Tomlinson had questions about the auditing and oversight components of the Use Policy, wanting to see more details about who manages that process. Additionally, she has concerns about data retention and management.

Chair Hofer asked for any public speakers:

There was one public speaker, Asada Olugbala, who suggested a performance audit of the PAC since it is reviewing many aspects of the police department and feels this is overstepping.

It was agreed that a smaller working group would continue to work with OPD and Forensic Logic to get a refined policy back to the group and return to the PAC.

ITEM 4

RICHARD AND RHODA
GOLDMAN SCHOOL
OF
PUBLIC POLICY
UNIVERSITY OF CALIFORNIA BERKELEY

Oakland Resident Data: Understanding What's Collected and Strengthening Privacy

Report prepared for:
Privacy Advisory Commission, City of Oakland

Report prepared by:
Antonio Flores | Jigyasa Sharma | Louis Au Yeung | Randy Clopton | Satoshi Miyano

May 18, 2020

RICHARD AND RHODA
GOLDMAN SCHOOL
OF
PUBLIC POLICY
UNIVERSITY OF CALIFORNIA BERKELEY

Table of Contents

RICHARD AND RHODA
GOLDMAN SCHOOL
OF
PUBLIC POLICY
UNIVERSITY OF CALIFORNIA BERKELEY

Acknowledgements

The report titled, "***Oakland Resident Data: Understanding What's Collected and Strengthening Privacy***" has been prepared by a team of graduate student consultants at University of California, Berkeley, Goldman School of Public Policy (GSPP). The report was prepared for the Privacy Advisory Commission of the City of Oakland. The analysis in this report follows the recent adoption of the seven Privacy Principles by the City of Oakland. The objective of this report is to identify the existing data practices of the City's departments and undertake a best practices analysis for the successful implementation of the Privacy Principles.

This report has benefitted immensely from excellent insights from: (1) Deidre Scott, Citywide Records Manager under Oakland's City Clerk's Office, who helped us streamline the department list and assisted in establishing communications with the departments; (2) Hector Dominguez, Smart Cities Open Data Coordinator for the City of Portland, who shared the experience of the City of Portland in implementing their own privacy program and principles. Mr. Dominguez also helped us think about the ground realities of implementing a privacy program and the resource constraints within which most local governments operate; (3) Nancy Marcus, City Administration Analyst in the Special Activities Permits division under Oakland's City Administrator Office, who helped us understand the status quo of the data and privacy practices at her department; (4) Kelsey Finch, Senior Counsel at the Future of Privacy Forum, helped us understand the experience of the City of Seattle and the general perception that local governments have towards privacy. Ms. Finch emphasized the need for viewing privacy as a dynamic and evolving policy problem. We are grateful for their willingness to share their knowledge with us and for taking time to talk to us during these extraordinary times of the COVID-19 pandemic.

This report would not have been possible without the constant support and encouragement from our project advisors from the Privacy Advisory Commission – Brian Hofer, Chair District 3 Representative, and Chloe Brown, District 2 Representative. We would also like to extend our deepest gratitude to our GSPP faculty coach Dr. Meredith Sadin. Dr. Sadin provided us with

guidance, feedback, and support throughout the length of the entire project, and helped us review and structure the report in its current shape. Finally, we are thankful to everyone in the City of Oakland, Joe DeVries (Chief Privacy Officer of the City), the GSPP community, and our family and friends for their support throughout the entire process, and for their flexibility and compassion amidst a global pandemic.

Antonio (Tony) Flores
Jigyasa Sharma
Louis Au Yeung
Randy Clopton
Satoshi Miyano

Master of Public Policy 2021
University of California Berkeley
Goldman School of Public Policy

Executive Summary

In recent years, personal data and information have become an increasingly valuable commodity. Personally Identifiable Information (PII) is collected every day by organizations such as social media companies, financial institutions, and government. With the volume of PII that is collected, the need for this information to remain private is stronger than ever. However, there are relatively few protections enshrined in the laws of the United States. The City of Oakland became a leader in the field of citizen data privacy after the passage of a set of Privacy Principles on February 2020. The Principles are designed to protect the data and privacy of Oakland's citizens, both within the city government and when data is shared with third parties. This report will focus on the best practices the City of Oakland should follow when implementing these Principles.

To craft these recommendations, our team drew on several key resources: a survey of Oakland's various administrative departments and divisions, interviews with employees of the City of Oakland, examination of similar privacy principle implementations in Seattle and Portland, and a series of interviews with leading privacy experts. As a result, we gained a number of key insights about Oakland's administrative structure and practices, the successes and challenges in Seattle and Portland, and how these lessons can be applied within Oakland's administrative departments. Based on those insights and our further research, our team recommends five specific practices designed to facilitate the smooth rollout of Oakland's Privacy Principles. These include:

Harmonizing the Needs of Stakeholders

Each department in the City of Oakland, Oakland's residents and businesses, and other citywide stakeholders all play a role in ensuring the privacy of Oakland's residents. It is important that each of these groups have a voice throughout the implementation process of the Principles. This means creating a clear structure of privacy in a centralized place within the City's organizational structure, such as the Office of the City Administrator. Individual departments should also have a say in how privacy may look and operate within their department. Likewise, departments may

have a rigorous central framework to begin with and it is important their experience and expertise be respected. Therefore, responsibilities should be gradually devolved over time. In addition, the public should have a say in how they view their data, and city administrators should keep a live dialogue with residents on how their data should be safeguarded.

Establishing "Privacy Champions"

Privacy champions, in this context, refer to individuals within departments who focus on implementing privacy within their local context. Champions should regularly interact to share expertise and discuss privacy practices with the Privacy Advocacy Commission (PAC) in order to facilitate strong practices and ensure the voice of each department is heard.

Providing Privacy Training

The City of Oakland should provide training to all employees on definitions and best practices for safeguarding resident's data. Different organizations offer such trainings, including the International Association of Privacy Professionals (IAPP). In addition, Seattle, Portland, and San Francisco have all provided training to employees which may serve as a model for Oakland.

Securing Resources

Oakland and PAC should outline a set of necessary resources in prior to implementing the Privacy Principles. This includes securing funding, understanding what particular departments may need, and finding manners of engaging the public to help craft privacy programs.

Auditing and Reviewing

The PAC should conduct regular audits of practices across all administrative departments. These audits should examine past and present practices and determine the best way to modify programs to lessen the impact on privacy concerns. The PAC should also conduct privacy impact assessments to evaluate the potential impact of future programs and practices on citizens'

privacy. At first, these should be conducted by experienced professionals, but over time some responsibility can be devolved to individual departments.

1. Understanding Privacy – Why Do we Care?

As the world continues to transition into the digital realm, issues of privacy and security continue to take center stage. The International Association of Privacy Professionals (IAPP) describes information privacy as "the right to have some control over how your personal information is collected and used." In this day and age of lightning-speed technological innovations, privacy is a continuously evolving complex concept with no universally accepted definition of what it entails.

The Organization for Economic Cooperation and Development (OECD) developed the Fair Information Practice Principles (FIPPs) in the 1970's. FIPPs were among the first internationally recognized privacy principles that served as privacy guidelines for the public and the private sectors across countries. Since then, these principles have evolved and have been infused in the privacy framework of several national and state governments around the world.

1.1. Privacy in the City of Oakland and Goldman School of Public Policy Consultant Group

Oakland is among the first cities in California to establish its own Privacy Advisory Commission (PAC) and subsequently adopt its own Privacy Principles. These Principles were drafted with the aim to safeguard every Oaklander's right to digital privacy and safety and will serve as the cornerstone for fair and ethical use of citizen data by the city departments.

As consultants to the PAC we approached personal privacy using the seven Privacy Principles that Oakland voted and passed on March 3, 2020.[1] Ensuring personal privacy requires, but is not limited to, equitable data management practices, proper collection and retention of data, and secure and transparent management of personal information. The Privacy Principles also apply to third-party relationships and data sharing protocols and requires public records disclosures and

[1] Refer to the seven Privacy Principles adopted by the City here: https://oakland.legistar.com/LegislationDetail.aspx?ID=4333053&GUID=CA379643-EE3A-4D17-A55D-759F3ECDE352&Options=&Search=

accountability. Before delving into the best practices for implementation of the Principles, we outline the privacy landscape in the United States and California to highlight the importance and need for adopting privacy principles at all levels of government.

1.2. Privacy in the United States

The United States of America has passed several federal data protection laws to protect the private and personal information of users, non-profits, and public and private institutions. To this date a comprehensive federal privacy law does not exist. Despite the many attempts to protect privacy, the definition and implication of privacy varies on a case-by-case basis. Therefore, privacy as a concept, legal right, and law is dependent on the type of regulation and personal information that is at hand.

For instance, the Federal Trade Commission considers data and information that can be linked or reasonably linkable to a person as personal data. This definition includes device identifiers and Internet Protocol (IP) addresses as personal data. Unauthorized access, usage, or sharing of this personal data would constitute a violation of privacy.[2] On the other hand, the constitutional "right to privacy" developed over the course of the 20th century protects Americans against government intrusions[3], but provides limited guidance and protection from private actors on the internet.

With the rise of internet usage and the public and private sector's ongoing transition into the digital space, defining and protecting privacy has become increasingly debated. Many private companies that collect data have ambiguous and constantly changing privacy and data policies. Often, these companies approach privacy and personal information through a more business-oriented lens and tailor their policies based on the products they provide to society. For example, Facebook, a social media and advertising company, reserves the right to use user

[2] "Definitions in United States." Data Protection Laws Of The World. DLA Piper, January 27, 2020. https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US.
[3] Mulligan, Stephen P., Chris D. Linebaugh, and Wilson C. Freeman. "Data Protection Law: An Overview." Congressional Research Service, March 25, 2019. https://fas.org/sgp/crs/misc/R45631.pdf.

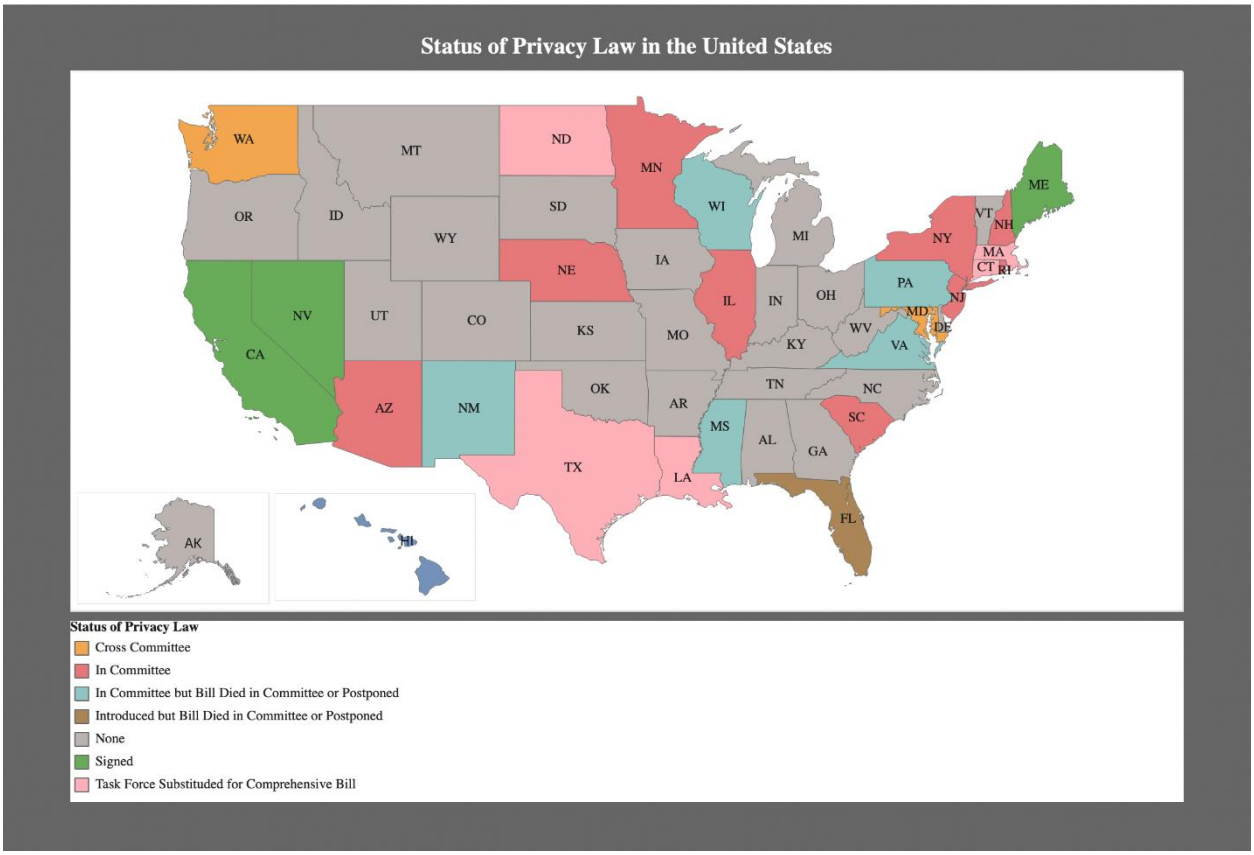
information based on what the company sees fit with their services and features. This includes, but is not limited to, collecting unique identifiers and Family Device ID's from the personal devices that are used to access Facebook's products. Thus, what constitutes privacy and privacy violations can also vary based on whether a consumer is willing to engage in particular internet platforms and whether they have agreed to a private company's terms and conditions.

State and local public governing bodies also uphold specific privacy practices that may be unique to their own location. For example, the state of Arizona prohibits libraries to disclose any personal and private information regarding a person's usage of publicly funded resources that are offered through the library. However, this law is limited to resources that are funded through taxpayer money.[4] It is unclear how the state's privacy laws apply to privately funded resources that are also available through the state's libraries. While public institutions may not approach privacy through a business lens, they face their own barriers in providing public goods that ensure the privacy of Americans.

As such, while Americans have become increasingly concerned about their personal privacy, the United States does not have a single definition, law or policy that can be used as a one-size-fits-all answer to privacy concerns. Rather, the U.S. protects privacy rights through several laws and pieces of legislation that are used in combination. The map below provides a comparison of State comprehensive-privacy law. The majority of States have no bill or statute for privacy rights for U.S. residents.

[4] "State Laws Related to Internet Privacy." National Conference of State Legislatures, January 27, 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

Figure 1:



Source: GSPP's data visualization of information provided by IAPP

1.3. Privacy in California

Personal data has been used as a commodity by many firms across industries. However, in recent decades, technology and social media companies have been the main drivers of increasingly integrating and depending on personal data for their products, services and business plans. Users of these products often have limited knowledge of how their data is used, though many companies make their data policies publicly available. Many also require authorization and consent before users can use their products.

Effective January 1, 2020, the California Consumer Privacy Act (CCPA) was viewed as a significant step towards ensuring consumer privacy rights for Californians. In the absence of a comprehensive federal privacy law, the CCPA draws from Europe's General Data Protection

Regulation (GDPR) and calls for transparency in data collection, usage, sharing and retention practices. CCPA defines personal information as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

The law gives Californians the right to (i) know what is being collected, (ii) know if their information is being shared and/or disclosed and to whom, (iii) refuse sale of their personal information, (iv) access their personal information, and (v) equal service and price even if they use their privacy rights. CCPA is however, nebulous in parts and has limitations. For instance, the law applies to both online and offline business practices. While notices for offline collection have been stated, it is unclear as to what extent these approaches to offline notices can be practiced and the type of data being collected will require these offline notices to begin with. Nevertheless, the law serves as the first and only one of its kind in the U.S. that provides extensive guidance on how to protect privacy.

Prior to CCPA, California's Online Privacy Protection Act (CalOPPA) and Children's Online Privacy Protection Act (COPPA) were implemented to protect and provide guidelines for secure online privacy practices for Californians. These policies continue to be used in California.

2. Understanding Client Setting

2.1. Organizational Structure of the City of Oakland

The City of Oakland operates under a mayor-council system of government. Certain top administrative officials, such as the City Administrator, are appointed by the mayor and subject to the approval of the Council. Others, including the City Attorney and City Auditor, are elected officials. One administrative official, the City Clerk, is appointed by the City Administrator, subject to approval of the Council. In addition to these officials, the City hosts a range of board and commissions such as the Privacy Advisory Commission (PAC)[5], which is comprised of privacy advocates and experts. PAC advices the City of Oakland on the best practices to protect Oaklanders' privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores citizen data.

The myriad of programs, functions, and services carried out by the city government are all overseen by the City Administrator's office. These programs are carried out by a number of departments which are then further divided into divisions that carry out individual directives within each department. Top-level departments include the Departments of Transportation, Public Works, Finance, Parks & Recreation, and many more. Divisions within these departments include the Purchasing division in the Finance department, the Recreation Centers within the department of Parks & Recreation, the Construction Management division in the Public Works department, and many more. As these departments operate at the direction of the mayor and city council, the departments do not directly report to the PAC, despite the commission's authority over the privacy practices that take place within the city.

The departments do not necessarily have mutually exclusive duties. Occasionally, departments will collaborate on certain projects or will share systems that operate for both departments. For example, the Transportation department and the Public Works department both manage contracts

[5] City of Oakland California, City Administration, Privacy Advisory Commission, http://www2.oaklandnet.com/government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm.

with outside entities through the Contract Services group. A full list of departments and their associated divisions can be found in Appendix 1, alongside a designation indicating which divisions currently collect citizen data as well as which divisions may share data.

2.2. Assessing Departments' Privacy Risks

While at least one division in each department collects some form of citizen data, the amount of data collected and the sensitivity of the data each division collects varies widely across different departments. With the assistance of Commissioners Hofer and Brown and Citywide Records Manager Deidre Scott, we compiled a list of relevant departments, with the duties of each department supplied by Ms. Scott. We then assigned each department a rating designed to indicate which departments may collect the largest volume or most sensitive data. Table 1 details these ratings, alongside a justification for each designation. Our team made use of these designations to focus our initial canvas of Oakland's data privacy landscape, and these designations may be useful to the PAC in the future. Under the direction of our project advisors from PAC, we excluded some departments with which the PAC has already developed a relationship, including emergency services such as the police and fire departments, as well as departments which either the PAC or Ms. Scott indicated have minimal interactions with citizens.[6] We were unable to meet with representatives of each department due to the ongoing coronavirus pandemic, our team does not know the full extent of what specific data indicators the department collects, nor the source of this data, and our understanding is limited to what little public facing information exists on Oakland's website and the information provided by Ms. Scott.

[6] Based on interview with Deidre Scott

Table 1: Departments' Probability of Encountering Privacy Challenges and Priority Designations

	Department	Rationale
High probability of encountering privacy challenges	Information Technology	The Information Technology Department designs and manages the IT system and mobile apps for the city. Many of the apps that are provided require residents to provide personal information. A lack of proper management of the data has the potential to compromise the safety and wellbeing of residents. Among the areas of high concern is the mobile app that allows residents to file complaints against the Oakland police through any smart device.
	Housing & Community Development	The department utilizes data mainly from census or other databases. The department also collects data as part of programs to assist with rent control, utility payments, and home purchases within the city.
	Finance	Deals with a significant amount of tax data from consumers and businesses, including tax identifiers and income information.
	Human Services	The department offers programs and as such they collect personal data from applicants, with some of those applicants being the elderly or belonging to the underprivileged class. They also deal with grant applications from organizations, so data from those organizations are collected as well. Grant applications have to be uploaded to a database run by Cityspan, a third-party.
	Planning & Building	Several key performance indicators used to track the performance of the department. However, no known personal data was collected. The public can submit concerns however it is unclear what data is being collected in the process.
	Transportation	The Transportation department has launched several programs designed to provide residents with different transportation options. These include e-scooters designed for residents with disabilities. It is important to ensure that GPS tracking data and personal health related information is not compromised by third-party partners such as Lime.

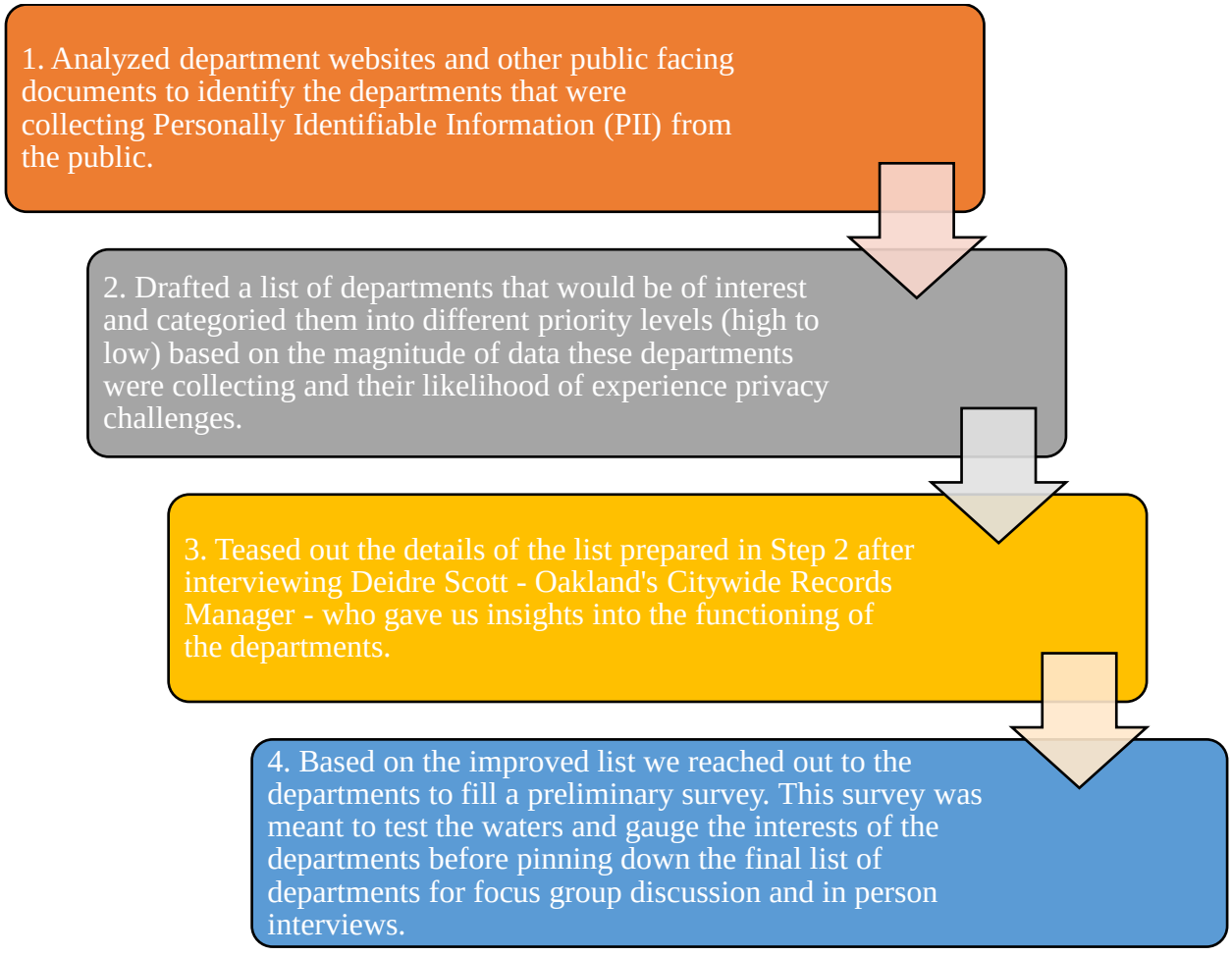
Medium probability of encountering privacy challenges	Parks, Recreation & Youth Development	The Recreation Centers and Youth Activities divisions collect data for participation in activities or use of the facilities.
	City Administrator	The City Administrator is the overarching operational and administrative body for all of the City's departments. Among their primary responsibilities, managing elections and political related initiatives is included. We are unsure of the extent to which they collect data, however it is worth looking into their role in managing all of the departments across the city.
	Public Ethics Commission	The Public Ethics Commission collects information on lobbyists and candidates for public office.
Low probability of encountering privacy challenges	Library	Certain services, such as issuance of library cards, require collecting a small amount of data.
	Contracts & Compliance	Collects data, including tax data, of businesses and data of the owners and employees. The employment referral service for construction workers collects the personal data of applicants, and applicants are required to consent to their sharing of information with other employment agencies.
	Economic & Workforce Development	Public dashboard for quarterly economic and development indicators ranging from employment and revenue to quality of life. No known personally identifiable information being collected.

3. Project Objective, Plan and Methodology

3.1. Objective and Plan

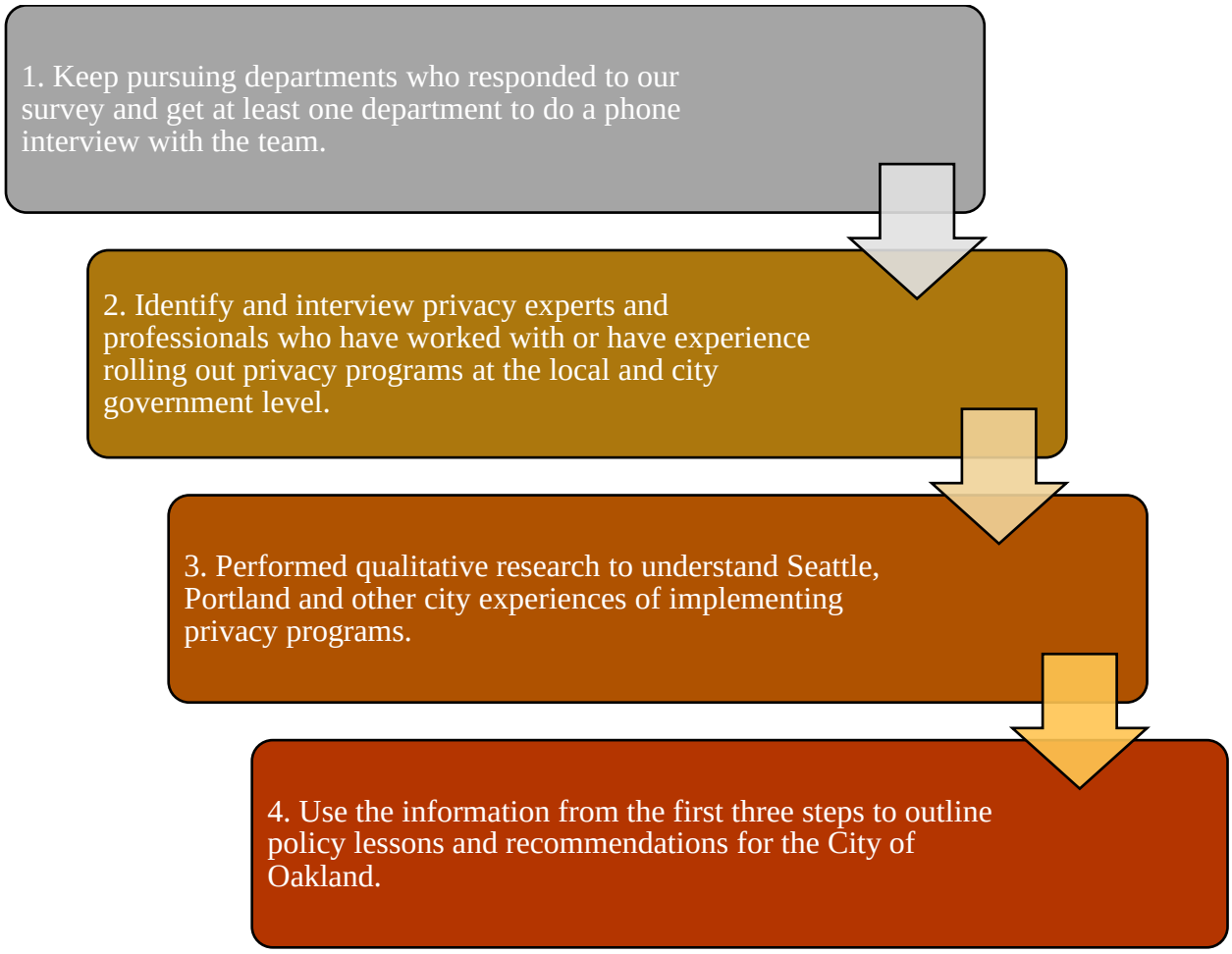
The objectives of our research are two-fold. First, understand the existing data and privacy practices of the city departments and second, outline best practices to implement the Privacy Principles across the City's departments. To achieve these objectives our team took the following steps:

Figure 2: Project Plan before COVID-19



Our plan took a hit as COVID-19 concerns escalated in the Bay Area. We managed to roll out the survey, however we received less than a 20% response rate. We devised an alternative plan that would fit in the new realities under COVID-19.

Figure 3: Project Plan after COVID-19



3.2. Methodology

3.2.1. Survey

With the guidance of Deidre Scott, Citywide Records Manager in Oakland, and our PAC and GSPP advisors, our team created a survey that included ten questions related to the data management and practices of each department (See Appendix 3). Our team hoped that at least

one employee from every division would complete the survey (See Appendix 1). This survey was created on SurveyMonkey and was e-mailed directly to 57 employees across divisions highlighted by Ms. Scott as points of contact.

3.2.2. Expert Interview

We interviewed different experts with professional backgrounds in privacy and/or local government. Experts represented two departments in the City of Oakland, the Smart Cities Open Data initiative in the City of Portland, and the Senior Counsel for the Future of Privacy Forum. Our conversation with the representative of Oakland's City Clerk's office was the only interview that was held in-person and was intended to help us gather specific information related to the operations of the City that we later used to tailor the survey we administered. The rest (3) of the interviews were done through Zoom meetings and phone calls. We followed the same general script for these interviews, though, each conversation ultimately varied from one another due to the different experiences and backgrounds of the interviewees (See Appendix 2 for the Interview Protocol).

With guidance from our academic and project advisers, our team got in contact and interviewed several experts who have extensive experience working in or with local government(s). Individual profiles and background summaries of each individual our team interviewed are listed below:

Table 2: Interviewee Profile

Expert	Organization	Background
Deidre Scott	City of Oakland	Deidre is the Citywide Records Manager for the Office of the City Clerk in Oakland. Ms. Scott oversees the management of department proposals across the City of Oakland and has extensive knowledge of the organizational structure of the City. Her managerial role makes Ms. Scott one of the few

		staff in the entire city with knowledge of the individual operational dynamics across the City's departments.
Hector Dominguez	City of Portland	Hector is the Smart Cities Open Data Coordinator for the City of Portland. Portland's Open Data initiative is meant to increase reporting, accessibility, and transparency of the City's data collection practices. Mr. Dominguez assists in creating strategic frameworks to improve the City's data governance, and actively works to assure the adoption and compliance of Portland's Privacy and Information Protection Principles across the City's departments.
Nancy Marcus	City of Oakland	Nancy is a City Administration Analyst in the Special Activities Permits division under Oakland's City Administrator Office. Ms. Marcus is responsible for processing cannabis, massage, and other niche business applications. Given the nature of her work, she has an extensive understanding of the importance of assuring equity and privacy as it relates to the City's management of highly sensitive information.
Kelsey Finch	Future of Privacy Forum	Kelsey is Senior Counsel at the Future of Privacy Forum. Ms. Finch is responsible for leading projects on smart cities, personal identifiable data information management, and ethical data sharing and research. Ms. Finch also has extensive experience in advising cities on how to develop and implement privacy principles that reflect the needs of the public.

3.3. Data Collection Limitations

Despite multiple nudges from our PAC advisors and our team, the response rate remained below 20 percent. Question 1 of the survey asked respondents to include their department and/or division, however, many individuals did not provide this information. With the help of our advisors and the information provided throughout the rest of the survey our team was able to identify some of the divisions and departments that were not mentioned. There were a few respondents whose divisions and/or departments were not identified.

Our interview with Ms. Scott was the only one that was in-person and took place prior to California's COVID-19 shelter in place mandates. We initially wanted to interview employees across each of the departments in the City of Oakland, however, the majority of individuals did not reply to the multiple interview requests we sent out. As a result, we shifted our focus to get in contact with Nancy Marcus, City Administration Analyst in the Special Activities Permits division under Oakland's City Administrator Office, whose work involves managing sensitive PII. For our analysis of the City's existing data practices, we use the information obtained from Ms. Marcus, however, the practices followed by her department may not be reflective of practices across different divisions.

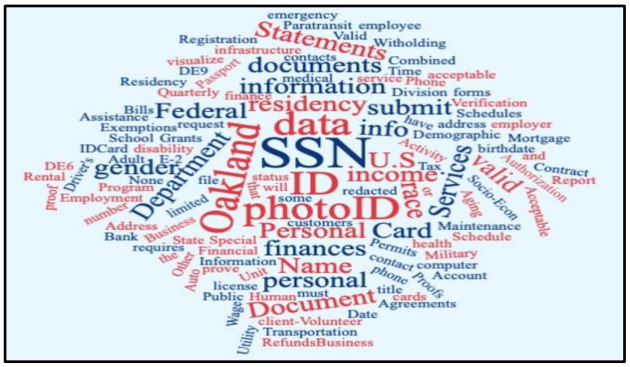
Given the low response rate from Oakland City employees and Seattle and Portland's more extensive experience with their own privacy principles, we believed that substituting interviews with experts in those cities who are further along their privacy initiative's timeline would serve of equal or greater value for our project.

4. Survey Results and Expert Interviews

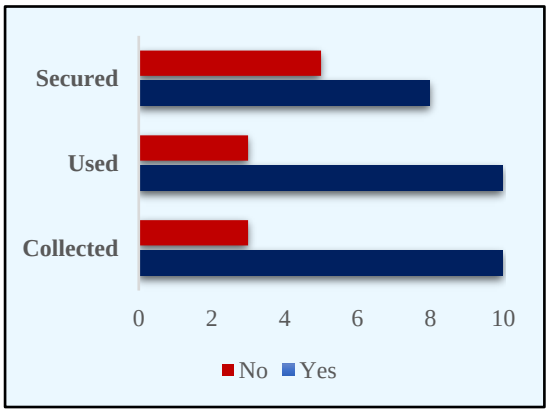
4.1. City of Oakland Survey

The objective of the survey was to get insights into City's data practices with regards to the following:

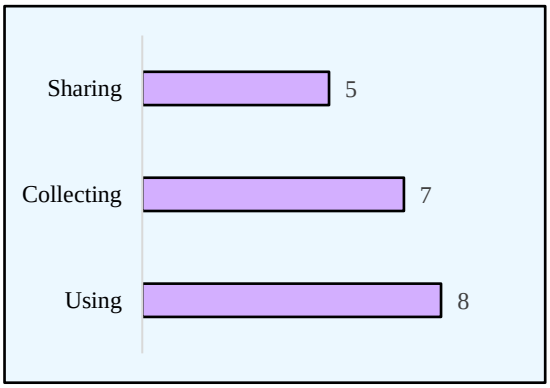
- **What's Collected?**
  - 10 out of the 13 divisions surveyed are collecting Personally Identifiable Information (PII)
  - Most commonly collected data was Social Security Number (SSN), photo ID, name, residency, gender, etc.



- **Is the Public Informed?**
  - Most departments inform the public on how their data is being collected, used and secured.

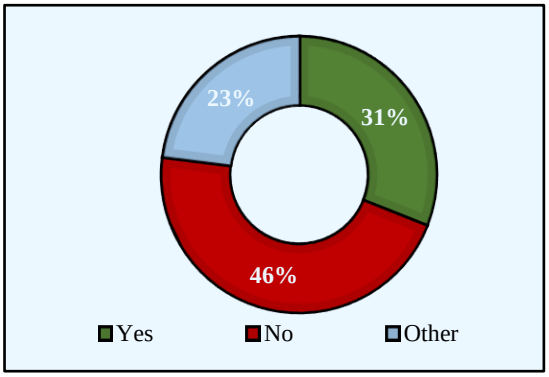


- **Is Public Consent Obtained?**
  - Only 2 divisions are sharing data, but 5 divisions noted that they are seeking consent from public before sharing data
  - Not all departments are seeking consent from public before collecting and using data.



- **Are the data collection practices transparent[7]?**

  - 46 percent of the divisions do not inform the public of its data collection practices on their website

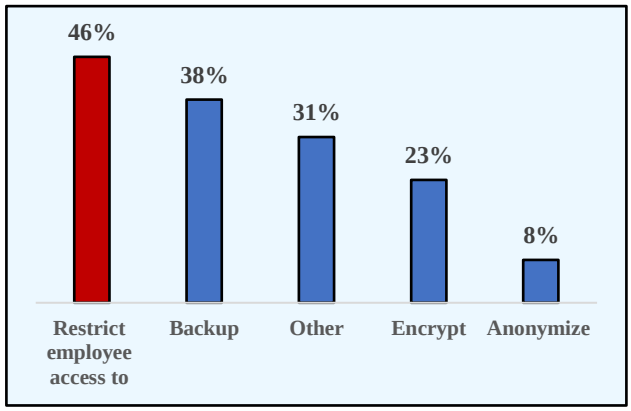


- **How is the data collected and stored?**

  - Most divisions are using more than one method of data collection and storage
  - **Paper forms** are the most common used method of collection and storage across departments
  - Second most common used method of data collection is on city owned devices

- **What data security measures are taken?**

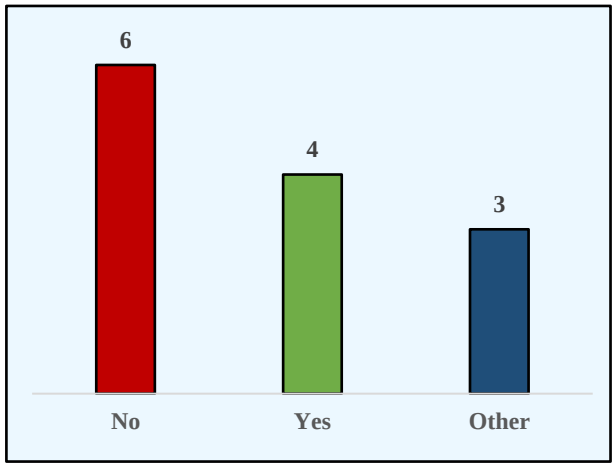
  - Most divisions use more than one method to secure their data



[7] Transparent refers to the stating the department's data collection practices on the department website.

- **Does the department have a designated data security and privacy personnel?**

  - 6 out of the 13 divisions surveyed do not have designated personnel to look after data and privacy practices



4.2. Findings from Expert Interviews

Overall, the findings from our interviews supplemented the data that we gathered from our survey and allowed us to meet several project objectives, including but not limited to: designing and administering a survey across departments in the City of Oakland, formulating an in-depth understanding of the organizational structure of the City of Oakland, and highlighting critical factors of success that are necessary to achieve the mission of the Privacy Principles. Our findings were incorporated into our recommendations for PAC that we provide later in the report. There were several recurring themes that we found throughout all of our interviews. We outline key themes below:

Theme	**Key Attributes**
Awareness and Transparency	• Early and ongoing department visibility is key to ensuring privacy practices are implemented and followed • Leveraging organizational networks will mitigate a lack of awareness of the principles and the likelihood of departments becoming siloed

	• Centralizing a chain of command provides clear lines of sight and resource for those who are unfamiliar with PAC or the principles
Networks and Accountability	• Early inclusion and conversations with city staff, city residents, privacy experts, and third parties will help create buy-in • Creating a network of department "privacy champions" will help reinforce principles • Open networks can solve issues that arise from limited resources by providing crowdsourced solutions • Generating networks can produce organic citywide cultural shifts and attitudes towards privacy practices • Build a relationship with each department
Practices	• Develop a one-size-fits-all framework of practices that departments can slot themselves into • Present a clear list of priorities that can be handled at the department level and those that would require escalating • Become a resource to the departments, with the eventual goal of devolving more responsibility for Privacy Impact Assessments to individual departments • Work within and around budgetary restrictions and schedules, consider the needs of departments when planning implementations
Training	• The privacy world is dynamic, keep abreast of changes in the landscape • Encourage departments to share their practices, experiences and expertise with one another • Take advantage and market IAPP trainings, City and County of San Francisco's Data Academy, and any number of training and workshops in the Bay Area

5. Best Practices, Opportunities and Challenges in Implementing Privacy Principles

5.1. Seattle's Privacy Principles and Relevance for Oakland

The City of Oakland is not the only city in the U.S. to establish a set of Privacy Principles. In Seattle, the City of Seattle Privacy Principles were adopted as a City Council Resolution in February 2015.[8] The City of Seattle established its privacy principles because of the greater opportunities for data collection due to the use of information technologies in administration and law enforcement, a belief that protecting the privacy of individuals who interact with the government is essential for maintaining public trust, and as a response to calls from civil society to review the City's privacy practices and develop a City-wide privacy policy.[9] It is also worth noting that the Privacy Advisory Commission of Oakland discussed Seattle's privacy initiative in October and November 2017 meetings, and there was talk of developing Oakland's privacy policy upon the Seattle model.[10]

Oakland's Privacy Principles share many similarities with Seattle's Principles. For example, both aim to limit the amount of data collection used for providing services to the public[11], stress the protection of personally identifiable information collected from the public, and seek to inform the public when they are collecting that information.[12]

[8] "About the Privacy Program." Seattle Information Technology. City of Seattle Information Technology. Accessed May 10, 2020. http://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program.
[9] "Res 31570 Version: 1." Office of the City Clerk. City of Seattle Office of the City Clerk, February 23, 2015. https://seattle.legistar.com/LegislationDetail.aspx?ID=2171323&GUID=21BBB334-AAC9-4904-8286-AB7C3CB783C4&Options=&Search=&FullText=1.
[10] "November 8, 2017 Special Meeting Agenda." City of Oakland. City of Oakland Privacy Advisory Commission. Accessed May 10, 2020. http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/agenda/oak067651.pdf.
[11] "About the Privacy Program." Seattle Information Technology. City of Seattle Information Technology. Accessed May 10, 2020. http://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program.
[12] "City of Seattle Privacy Principles." City of Seattle. City of Seattle. Accessed May 10, 2020. https://www.seattle.gov/Documents/Departments/InformationTechnology/City-of-Seattle-Privacy-Principles-FINAL.pdf.

5.2. Portland's Privacy Principles and Relevance for Oakland

The City of Portland has been part of the national effort to create "smart cities" that operate on better data and automation. The City of Portland collects and manages data that may put communities, individuals or sensitive assets at risk. This includes the data about residents on city street, sidewalks, and even in their own homes.

The City of Portland adopted the Privacy and Information Protection Principles on June 19, 2019.[13] The principles provide guidelines for protecting private and sensitive data managed by the City of Portland or those working on behalf of the City of Portland. A lot of the City of Portland's principles are based off Seattle's model.

At this point, Portland's implementation of its Privacy Principles is still in its early stages, and the City is working with other city bureaus and communities to implement the principles. The Smart City PDX team, which is one of the major drivers of this privacy initiative, is partnering with the Office of Equity and Human Rights (OEHR) and other City agencies and bureaus to coordinate an internal Privacy Work Group focused on implementation. The work group will identify short-term and long-term policies and procedures for implementing and upholding the Privacy Principles. Other objectives of the work group include identifying strategies for community involvement during implementation, as well as the identification of resources to sustain this work and make it successful. [14]

5.3. Lessons from the City of Seattle

Oakland and Seattle share the need for city departments to act upon the Privacy Principles. In Seattle's case, the city rolled out a Privacy Policy in July 2015 that informed all departments about their obligations to follow the Principles[15], including providing notice about the collection,

[13] Dominguez, Hector, Judith Mowry, Elisabeth Perez, Christine Kendrick, and Kevin Martin. "Privacy and Information Protection for a New Generation of City Services." *Proceedings of the 2nd ACM/EIGSCC Symposium on Smart Cities and Communities - SCC 19*, 2019. https://doi.org/10.1145/3357492.3358628.
[14] Ibid.
[15] "About the Privacy Program." Seattle Information Technology. City of Seattle Information Technology. Accessed May 10, 2020. http://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program.

use and sharing of personally identifiable information, adhering to the city's data retention schedule, and maintaining documentation for evidence of compliance to the Principles.[16]

The City of Seattle has tried to facilitate the departments' implementation of the Privacy Principles through organizational changes and creating processes and tools. For example, a Privacy Office under the Information Technology department was created in 2015 to support City departments in meeting the Privacy Policy. After convening a group of representatives from 15 departments to create policies and practices, the Privacy Office designed a citywide Privacy Program to provide guidance and tools to City employees when they work with personally identifiable information. The Privacy Office provides annual privacy training for City employees, conduct privacy reviews on technologies used in new and existing City programs across all departments and carries out advocacy work.[17] Since September 2017, the Privacy Office has carried out more than 2,000 privacy reviews and in 2019, it provided annual privacy training to around 12,000 City employees.[18]

The City of Seattle also decided to implement a departmental Privacy Champion program, where the Privacy Champion will provide department support for incorporating the Privacy Program objectives into systems and processes, such as handling basic inquiries, carrying out risk reviews and building awareness about privacy. Those Privacy Champions provide a network of focal points on the department level to promote the Privacy Program.[19]

The City of Seattle also created processes and a toolkit to help departments implement the city's privacy principles. According to the city's Privacy Program, owners of projects carry out a three-step privacy review process to determine the project's level of privacy risk and steps to mitigate

[16] "Privacy Policy." City of Seattle. City of Seattle, July 21, 2015. https://www.seattle.gov/Documents/Departments/InformationTechnology/privacy/PrivacyPolicyFINAL.pdf.
[17] "City of Seattle Privacy Program 2019 Annual Report: Transforming Privacy." City of Seattle. City of Seattle Privacy Office. Accessed May 10, 2020. http://www.seattle.gov/Documents/Departments/Tech/Privacy/2019 Privacy Program Annual Report.pdf.
[18] Ibid.
[19] "City of Seattle Privacy Program." Community Technology Advisory Board. City of Seattle Information Technology, October 2015. http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf.

those risks. The initial step is completing an assessment questionnaire, and if the answers indicate a low privacy risk, then project owners can use the resources provided in toolkits to handle the risks. For projects determined to have a higher privacy risk, the project owners will further respond to a Privacy Threshold Analysis where the departmental Privacy Champion will review the answers to determine whether the project owners can use the toolkit resources to handle the risk or an even more in-depth privacy review is required. For projects determined to represent a significant privacy risk, project owners complete a Privacy Impact Assessment which takes a more detailed look at projects to determine all potential impacts and options for mitigation.[20] The aforementioned toolkit that departments can refer to is an online collection of resources including process documents, review forms, training and awareness links and contract language that department employees can make use of to incorporate privacy principles into daily operations. [21]

5.4. Lessons from the City of Portland

Portland's case shows us that building up relationships among stakeholders is vital for successful implementation of privacy principles. The city realized that finding a way to bridge the gap between departments is the biggest challenge for the city since many departments are often very busy and siloed. The city tackled this problem by setting up a privacy workgroup to facilitate communication among departments. [22]

Another key takeaway for Oakland is the importance of public trust. Portland puts emphasis on addressing the issue of equity and recognizes that one of the wins has been around public trust. This was due to Portland actively talking about the relationship between citizens and city organizations and also because the community recognized that Portland's efforts were beneficial. [23]

[20] Ibid.
[21] Ibid.
[22] Based on interview with Hector Dominguez.
[23] Ibid.

6. Policy Recommendations

Based on the review and analysis above, we have devised a set of recommendations that Oakland should consider when rolling out the City's Privacy Principles. These recommendations constitute a set of best practices that PAC should keep in mind as they begin to introduce the Principles to each department and begin to craft a set of rules and regulations to create a culture of privacy within Oakland's city departments. These recommendations are not directives for how to implement privacy principles, but rather a set of tools to help avoid major challenges while the PAC follows its roadmap to roll out the Principles. We propose a set of five recommendations, focusing on engaging stakeholders, creating a network of local privacy experts, training staff, acquiring resources, and evaluating department progress and activities.

6.1. Harmonize the Needs of Stakeholders

Across all of our data sources, one particular theme stood out: the process of creating privacy practices cannot be conducted in isolation. In order to properly understand how to implement Oakland's privacy principles, the PAC must engage all stakeholders and those who would be affected by these principles. This includes actors within the city government and outside actors such as individuals, communities, and businesses. Creating an effective and comprehensive system of privacy practices requires an understanding of how each of these communities' view and define privacy as well as an understanding of how these practices can be incorporated into existing paradigms and frameworks.

6.1.1. Department-Level

Securing buy-in from each department within the city is a crucial element of ensuring that departments feel they can implement these practices without fundamentally uprooting their function. Kelsey Finch of the Future of Privacy Forum suggests allowing individual departments a degree of autonomy in order to be more effective in implementing privacy practices.[24] This

[24] Based on interview with Kelsey Finch.

should be done in collaboration with experts at the city level in order to ensure department practices remain harmonious with practices implemented citywide. The City of Seattle took a similar approach in the early stages of implementing their privacy principles to great success.[25] The City of Portland took a similar approach in the early stages of exploring implementation of their own principles, largely based on Seattle's model. After the passing of the principles, Portland's Smart City PDX team further coordinated a temporary privacy work group whose function is to serve as an advisory role to the City of Portland's overall data governance efforts. The work group included 14 agencies and bureaus in the City of Portland, for example the Portland Water Bureau, Bureau of Human Resources and Office of Equity and Human Rights. [26] According to Hector Dominguez, the Smart Cities Open Data Coordinator for the City of Portland, those bureaus were enlisted in the work group because the privacy risk they faced was most acute.[27] The work group's objectives include developing implementation processes and evaluating resources needed for successful long-term implementation, defining critical and short-term issues and ways the group can develop the policies or procedures to address them, understanding and documenting the current privacy and information protection practices in the City of Portland and recommending a privacy governance structure.[28]

Although bringing together departments in a group may facilitate communication and increase understanding of the needs and situation of individual departments, Mr. Dominguez acknowledged that this was not enough to overcome the silo-condition that the bureaus in Portland operated in. To further promote cooperation between the bureaus and the Smart City PDX and as a way to promote privacy awareness despite the coronavirus crisis disrupting original plans, Mr. Dominguez said that the Smart City PDX changed tack and distributed easy-to-read handouts and provided accessible information to bureaus. The Smart City PDX also

[25] Ibid.
[26] Dominguez, Hector, Judith Mowry, Elisabeth Perez, Christine Kendrick, and Kevin Martin. "Privacy and Information Protection for a New Generation of City Services." Proceedings of the 2nd ACM/EIGSCC Symposium on Smart Cities and Communities - SCC 19, 2019. https://doi.org/10.1145/3357492.3358628.
[27] Based on interview with Hector Dominguez.
[28] Dominguez, Hector, Judith Mowry, Elisabeth Perez, Christine Kendrick, and Kevin Martin. "Privacy and Information Protection for a New Generation of City Services." Proceedings of the 2nd ACM/EIGSCC Symposium on Smart Cities and Communities - SCC 19, 2019. https://doi.org/10.1145/3357492.3358628.

thought about and focused their attention on what kinds of projects and services that they could provide immediately in the crisis. One such service was providing initial privacy assessments for bureaus who were coming up with all sorts of measures to respond to the coronavirus. [29]

6.1.2. City-Level

Oakland faces an organizational hurdle similar to Portland: both have city departments that operate relatively independently. Thus, Oakland will need to consider its organizational structure when harmonizing practices across departments. Ms. Finch provided guidance on Seattle's approach to centralizing practices. Seattle housed its primary privacy oversight responsibilities in the relatively centralized Information Technology department. This allowed the IT department to place Seattle's practices into high visibility with a clear chain of command. [30] While Oakland's IT department is not similarly situated, the City Administrator's office plays a similarly central role in Oakland's organizational structure. We recommend that, when rolling out privacy practices and creating a culture of privacy, the PAC should collaborate extensively with the City Administrator's office to construct a clear framework that can be ported to each department from a higher authority.

In addition to centralizing enforcement within a central organization, the PAC and the City Administrator's team should also create a clear set of guidelines for triaging privacy concerns. As mentioned above, on recommendation from Ms. Finch, individual departments should keep some degree of autonomy over their practices. However, there are some issues that cannot be handled by individuals with only expertise in their own field. Ms. Finch recommends that a centralized privacy organization should establish clear guidelines for escalation of issues should citizens' privacy be threatened. Over time, this framework can be modified to devolve more responsibility as departments become more familiar with their own practices. [31]

[29] Based on interview with Hector Dominguez.
[30] Based on interview with Kelsey Finch.
[31] Ibid.

6.1.3. Understanding Public Needs

Finally, Oakland will need to consider the needs and issues within the communities these privacy principles ultimately serve. Public interaction is most important when considering the equity principle, as the experiences from impacted communities is vital to understanding how data collection practices may unfairly marginalize vulnerable communities. Mr. Dominguez emphasized that the relationship the Smart City team developed with citizens flew in both directions. Portland hosted a series of different community information sessions to inform the community of existing practices and gain feedback on practices from community members. Mr. Dominguez stressed the importance of targeted universalism (or the implementation of universal goals via targeted processes) as the key philosophy behind community interactions. Portland's Smart City team made an effort to trace an understanding of the data process all the way to its point of origin with individuals to fully understand how the privacy process affected each member of the community. Portland also made use of crowdsourcing in order to bring public stakeholders into the decision-making process. For example, Portland recently hosted a hackathon to bring the public into the process of equitable facial recognition software privacy. [32]

6.2. Creating "Privacy Champions" at The Department Level

Because so much data is currently available from a wide range of sources and databases can be transformed and combined, data that might not be considered as personally identifiable information may nonetheless identify individuals or allow inferences to be made about them.[33] As such, effective management of privacy at a city-level requires a diverse team that is represented by different departments, is capable of considering privacy in connection with every decision regarding data, and can work together to avoid sensitive information falling through the cracks due to the diversity of privacy risks.[34] Because of this, and also to ensure and ease the adoption of privacy principles in departments in the City of Oakland, it is worth exploring

[32] Based on interview with Hector Dominguez.
[33] Green, Ben, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford. "Open Data Privacy." Berkman Klein Center for Internet & Society, 2017.
[34] Ibid.

whether designated personnel could be assigned to be the person responsible for privacy matters in that department.

In proceeding with implementation of privacy principles, the City of Seattle implemented a departmental Privacy Champion program, where such privacy champions provide department support for incorporating the city's Privacy Program objectives. In Seattle, that responsibility was designed to be a part-time supportive function that is in addition to a person's regular job responsibilities, and responsibilities included handling basic inquiries, conducting and signing off low-risk reviews and validating response appropriateness in privacy assessments, actively participating in privacy meetings and building awareness about privacy. These departmental privacy champions are managed by and coordinate with the Privacy Program Manager, which is a full-time position in the department responsible for carrying out Seattle's privacy program. [35]

On the other hand, Portland's view on privacy champions presents a different story. Mr. Dominguez cautions that, while he is in agreement with the use of privacy champions, imperfect implementation could create a separation between the needs of the city as a whole and the needs of individual departments. [36] It is also worth noting that Ms. Finch instead suggests that these positions be compensated and resourced appropriately in recognition of their additional responsibilities within and across departments. [37]

6.3. Training and New Practices

Nancy Marcus, who works at Oakland's City Administrator Office, mentioned that when she was hired, knowledge and information about data management, cybersecurity or any other technology concerns were passed on only verbally and there was only one resource document regarding privacy. She also mentioned there is a slow standardization of these procedures.[38]

[35] "City of Seattle Privacy Program." Community Technology Advisory Board. City of Seattle Information Technology, October 2015. http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf.
[36] Based on interview with Hector Dominguez.
[37] Based on interview with Kelsey Finch.
[38] Based on interview with Nancy Marcus

These opinions point to a need for standardized training and more written learning materials for department employees if Oakland wishes for an across-the-board implementation of privacy principles. In this regard, it is worth looking to how Seattle and Portland have been providing the training and resources to their city employees.

In Seattle, such training is run by the Privacy Office, which provides annual privacy training for City employees via online channels. For the year 2019, more than 11,000 city employees completed the online Privacy and Security course, and the course had a 94% completion rate, with the majority of training completed in May, June and July. The Police Department, Seattle City Light, Parks and Recreation, Seattle Public Utilities and the Fire Department each assigned more than 1,000 of its employees to take part in the training.[39] Seattle also provides a privacy toolkit that contains resources that departments can refer to. The toolkit is an online collection of resources including process documents, review forms, training and awareness links, standards and policies, translations of privacy documents and contract language that department employees can make use of to incorporate privacy principles into daily operations. City departments whose applications, processes or programs collect the public's personal information need to be familiar with and use the resources in the toolkit. [40]

For the City of Portland, one of the objectives of the temporary privacy work group coordinated by Smart City PDX that consisted of city agencies and departments is to create some initial privacy impact assessment tools, which will include factors such as risk management, community engagement, transparency and accountability. Such tools are envisaged to help guide city staff to apply the City of Portland's privacy and information protection practices to their work in the short-term. [41] Mr. Dominguez mentioned that the City of Portland is looking to see

[39] "City of Seattle Privacy Program 2019 Annual Report: Transforming Privacy." City of Seattle. City of Seattle Privacy Office. Accessed May 10, 2020. http://www.seattle.gov/Documents/Departments/Tech/Privacy/2019 Privacy Program Annual Report.pdf.
[40] "City of Seattle Privacy Program." Community Technology Advisory Board. City of Seattle Information Technology, October 2015. http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf.
[41] Dominguez, Hector, Judith Mowry, Elisabeth Perez, Christine Kendrick, and Kevin Martin. "Privacy and Information Protection for a New Generation of City Services." *Proceedings of the 2nd ACM/EIGSCC Symposium on Smart Cities and Communities - SCC 19*, 2019. https://doi.org/10.1145/3357492.3358628.

how their human resources units can provide training to city employees, and is looking at models of training, such as San Francisco's Data Academy model. [42] In addition, both Mr. Dominguez and Ms. Finch mentioned trainings offered by the IAPP as valuable resources for training on different elements of privacy management.[43]

Lastly, it is crucial to remember that as technology advances and evolves, so does the need for privacy considerations. Consequently, actors within the city of Oakland will need to keep abreast of evolutions in the world of technology and the impact that new technologies will have on citizens' privacy, as well as brainstorm methods to curtail the privacy concerns brought about by new technologies.

6.4. Sourcing for Necessary Resources

According to the roadmap drafted by the PAC, it is expected that implementation of the Oakland privacy principles will require additional staff time and that additional City staff will need to be allocated to work with the Chief Privacy Officer and the PAC.[44] This will likely increase the need for fiscal resources. Mr. Dominguez has provided insights about the budget problems his team in Portland has faced, which is that resources and funds that his team requires now can only be allocated in the next budget cycle. [45] Based on that experience it is perhaps worthwhile for Oakland to plan ahead and ensure resources that will be needed to implement the privacy principles can be allocated in a timely manner.

At the same time, not all resources and material to promote privacy need to come from the city's coffers. For example, Mr. Dominguez mentioned that Portland turned to crowdsourcing to come up with material that focuses on accessibility to information. He also mentioned that there are also open-source resources. With respect to engaging minority communities, Mr. Dominguez

[42] Based on interview with Hector Dominguez.
[43] Based on interview with Hector Dominguez and Kelsey Finch.
[44] "Agenda Report: Adoption of Citywide Privacy Principles." City of Oakland California. City of Oakland, April 3, 2020. http://oakland.legistar.com/gateway.aspx?M=F&ID=2e6bff25-791a-4298-abe5-538d632548b2.pdf.
[45] Based on interview with Hector Dominguez.

found it more useful to leverage existing community networks and figures such as trusted leaders in the community to build that rapport, compared to just reaching out as a sole effort by his group. [46]

6.5. Regular Auditing and Review

In order to achieve the directive of safeguarding individual privacy while respecting the principle of open government and transparency and complying with public records disclosure requests, it is necessary to conduct regular audits and reviews of data privacy practices in the City of Oakland. As technology is constantly evolving and more and more datasets are made public by various parties, information and data that previously could not lead to personal identification may be used to identify individuals in the future. For example, more powerful reidentification techniques may be developed or information may be linked across old and new datasets that increases the possibility of reidentification. Moreover, the public may have changing perceptions of privacy or different attitudes towards government holding data as time passes. As such, it is important to undertake periodic auditing of data and processes to ensure privacy principles continue to be upheld. [47]

The audit should review the past and present and also be forward-looking at the same time. For example, when examining the existing datasets held by the City, questions may be asked of what is the current risk assessment of each dataset, what are the new forms of reidentification techniques that have emerged since the previously audit, and what datasets from other sources have been made public that could be linked to data that the city provides to the public. When looking at the process component of implementation of the city's privacy principle, the audit may include looking at whether every task is covered by someone with the relevant expertise and experience and considering what shifts in personnel have occurred or how the organizational structure of the City has changed. In examining the public's response and attitude to the City's

[46] Ibid.
[47] Green, Ben, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford. "Open Data Privacy." Berkman Klein Center for Internet & Society, 2017.

privacy principles, the audit could review how effective public engagement has been and incidents of negative feedback from the public or privacy scandals from other jurisdictions that could possibly influence public trust related to data. [48]

Ms. Finch also stressed the importance of privacy impact assessments. These assessments should evaluate new programs on their potential to impact citizens' privacy and should include assessments of the program's risk to citizen privacy, methods to mitigate privacy-related consequences, and considerations for human rights and equity impacts of programs. Initially, these impact assessments should be conducted by expert auditors selected by the PAC, but as time and experience evolve, these responsibilities could be devolved to individual departments. Training from the IAPP will be instrumental in this devolution process. [49]

6.6. Conclusion

Despite setbacks due to the ongoing pandemic, we believe that the five recommendations we presented still represent a solid set of guiding principles for the City of Oakland to abide by while implementing the privacy principles. While we were only able to collect minimal data from city employees, what data we were able to collect afforded us the ability to develop our five recommendations when paired with expert interviews and research on practices in other cities. In addition, we feel that our recommendations of remaining attentive to stakeholder needs, assembling local teams of privacy champions, and keeping abreast of resources requirements, department level needs, ongoing practices, and emerging trends can act as a model for other cities in the United States. We feel that our recommendations provide a solid groundwork for any city as these best practices were gathered from existing expertise alongside Oakland-specific data. In this way, Oakland may be able to serve as a model for effective implementation of privacy principles as more American cities begin to take citizen data privacy concerns to heart. As a pioneer in the field, this is one of many ways Oakland can lead the way in protecting Americans from the ever-encroaching specter of misuse and overuse of citizen data.

[48] Ibid.
[49] Based on interview with Kelsey Finch.

Appendix 1

Below is the contact list for the departments and divisions across the City of Oakland. The bolded text in the left column display the department name and the listings below that are the divisions within each department. It must be noted that this table was sourced through the City Clerk's office and it may not provide up to date information on each division's data collection and sharing policy.

Animal Services	**Contact**	**Collects Data**	**May Share Data**
Administration			
Field Services	Eugenia Taulealo	x	
Veterinarian			
City Administrator			
Administration			
Agenda			
Communications			
Contracting	Vivian Inman	x	
EOPD			
Nuisance Abatement	Susan Vasquez	x	x
Oakland Army Base			
Race and Equity			
Special Activity Permits/Cannabis	Nancy Marcus	x	x
Office of the City Clerk			
Administration			
Agenda	Asha Reed	x	
Elections & Compliance	Krystal Sams	x	
KTOP			
Records			
Economic Workforce Development			
Administration			
Marketing			
Economic Development			
Business Improvement Districts	Maria Rocha	x	
Recycling			

Business Assistance Center	Juno Thomas	x	
Real Estate			
Public/Private Development			
West Oakland Job Resource Center	Honorata Lindsay	x	
One Stop Career Center	Enjema Hudson	x	
Day Laborer Program	TBD	x	
Special Events/ Film Programs	Jim MacIlvaine	x	
Cultural Funding Program	Denise Pate	x	
Public Art Program			
Finance			
Administration			
Accounting			
Purchasing	Fred Haliburton	x	
Budget			
Audit/Compliance	Phillip Lim	x	
Business Tax	Rosana Munoz	x	x
Citywide Collections	Danita Lee	x	
Parking Citation Assistance Ctr	Brenda Fransaw	x	
Citywide Liens/Mandatory Garbage	Nicole Welch	x	x
Payroll			
Retirement			
Treasury			
Fire Services			
Administration			
Administration (Chief)			
Emergency Management Services			
Fire Prevention	Annete Boulware	x	x
Medical Services			
Housing and Community Development			
Administration			
CDBG/Commercial Lending			
Housing Assistance Center	Azaria Bailey-Curry	x	

Housing Development/1st Time Ownership	Angelica Patrick	x	x
Fiscal Administration			
Rent Adjustment	Maxine Visaya	x	x
Residential Lending/Rehab	Marchelle Huggins	x	
Human Services			
Administration			
ASSETS			
Community Action Partnership (OCAP)			
Community Housing Services	Blanca Leggett	x	
Fiscal			
Head Start	Thea Hernandez	x	x
Multipurpose Senior Services (MSSP)	Mary Albright	x	
Oakland Fund for Children & Youth (OFCY)	Carina Lieu	x	x
Oakland Paratransit (OPED)	Hakeim McGee	x	x
Oakland Unite			
Payroll			
Safe Walk to School/Summer Food	Carmela Chase	x	
Senior Centers	Scott Means	x	
Senior Companion/Foster Grandparent	Andrea Turner	x	x
Youth Leadership & Development	Sandra Taylor	x	
Information Technology			
Administration	Tyehimba Jelani	x	
Public Safety Systems			
Library			
AAMLO			
Branch Services	Derrick DeMay/Jenera Burton	x	
Children's Services	Nina Lindsay	x	
Financial & Administrative Svcs			
Main Services			

Parks, Recreation, & Youth Development			
Accounting			
Administration			
Aquatics	Harith Aleem	x	
Boating	Sarah Herbelin	x	
Central Reservations	Zermaine Thomas	x	
Contracts			
Payroll			
Recreation Centers	Harith Aleem	x	
Special Projects			
Sports (1)			
Sports (2)			
Planning & Building			
Administration			
Cashiering Operations	Diana Rex/Jonathan Arnold	x	x
Fiscal			
Inspection & Code Enf Administration	Traci Campbell	x	x
Permits, Building/Engineering & Plan Check	David Guillory	x	x
Landmark Preservation			
Planning & Zoning Service Counter	Robert Merkamp	x	x
Strategic Planning			
Public Ethics Commission			
Administration			
Enforcement	Ana Lara-Franco/Suzanne Doran	x	
Public Works			
Administration			
Fiscal			
Human Resources and Training			
Business & Information Analysis			
Public Information			

311 Call Center	Sabrina Jones	x	x
Sanitary Sewer Improvements			
Storm & Watershed			
Contract Services	Calvin Hao/Tamala Barnes	x	
Project Delivery			
Construction Management			
Construction Management & Material Testing			
Project and Grant Management		x	
Drainage	Gerald Nervis/Christian Lagassee	x	x
Facilities Services			
Heavy Equipment & Auto Shop			
Infrastructure Maintenance (Storm Drains & Sanitary Sewer)			
Keep Oakland Clean and Beautiful			
Environmental Services	Daniel Hamilton/Chris Staller	x	
Parks			
Tree Services	David Moore/Cecilia Garcia	x	
Transportation			
Director's Office			
Support Services/Administration			
ADA Programs			
Human Resources			
Fiscal			
Safety Training			
Capital Projects			
Right of Way	Kevi Kashi/Patrick Taylor	x	x
Parking Permits	Kevi Kashi/Patrick Taylor	x	

Paving and Sidewalks			
Survey			
Complete Street Design			
Planning and Project Development			
Great Streets (Infrastructure) Maintenance			
Streets and Structures			
Streets/Sidewalks			
Safe Streets			
Parking Meter Repair			
Bicycle Pedestrian Program	Jason Patton	x	x
Traffic Safety	Susan Kattchee	x	x
Complete Street Maintenance (Traffic & Parking Meters)			
Traffic Signal			
Street Lighting			
Taxi (Parking)	Michael Ford	x	x
Parking Enforcement	Michael Ford	x	
Mobility Management	Danielle Dai	x	

Appendix 2

Appendix 2.A.

General interview script with City of Oakland Officials. The questions listed, or a similar variation of it were asked during the interview. Based on the conversation and responses to some of the questions listed below, additional questions were asked but are not listed.

Data Collection and Use		
1.	For what purpose is your department collecting personally identifiable information (PII)?	(keep general, no specific indicators)
2.	What are the different ways in which the department is collecting PII?	
2(i).	How frequently is the data being collected?	
3.	Is the department considering any alternative methods to collect data?	If yes, go to Q3(i); if not jump to Q4
3(i).	What are these alternative methods? For instance – if the department has been collecting data through paper forms and plans to move to online surveys.	
4.	Is your department collecting data that could disproportionately affect racial minorities, disabled or low-income individuals?	If yes, go to Q4(i) and Q4(ii); if not jump to Q5
4(i).	How is this data being collected?	
4 (ii).	Why is the department collecting this data?	
Data Storage, Retention and Sharing		
5.	Where is the department storing data?	Probe for digital & physical storage. Such as on local drive, third party server or paper etc.
6.	How long is the data kept? Why?	
7.	Does your department share data with other departments or third parties?	If yes, go to Q7(i) and Q7(ii); if not jump to Q8
7(i).	What data is being shared?	

7(ii)	Why is the data being shared?	
8.	Are there any protocols for data sharing?	
9	What requirements or guidelines do you have for third parties that use your data?	
Interactions with the Public		
10.	What is your department doing to inform the public of your data collection, usage, management and sharing practices?	
11.	How does your division handle requests from individual citizens to have their data removed from your records?	
Data Privacy Policies		
12.	Who manages your division's data practices?	
13.	How does the department ensure privacy of individuals with respect to public record requests?	
14.	What sort of training does your staff receive regarding data management?	
15.	Tell us more about the data security measures adopted/practiced by your department.	

Appendix 2.B.

General interview script with Experts. The questions listed, or a similar variation of it were asked during the interview. Based on the conversation and responses to some of the questions listed below, additional questions were asked but are not listed.

Introductions
1. Permission to record and to be quoted directly or indirectly in our report.
2. GSPP Introductions
3. Can you share a little about your work with local governments and/or privacy?

Inside Scoop
4. Process - where are you in the implementation phase? (If they are not City Employees, ask about their previous experience with implementation)
5. Training, knowledge, how much do people really know? Who was responsible for disseminating knowledge?
Successes
6. What have been some positive outcomes?
7. What are some key factors that led to the successful implementation of the principles across city departments? (maybe prime for individual strategies and successes)
8. What were the organizational characteristics that helped facilitate the smooth implementation of the principles?
9. Can you talk about what resources - in terms of training, guidelines - that were provided to the city personnel across the departments prior or during the implementation of the principles.
10. What were some of the actions you took as an individual in your capacity to help bring about this success?
Challenges
11. There is some work that talks about the importance of creating a privacy culture at the workplace. In the case of Portland what did you or what are you doing to bring about that shift in the work culture?
12. How do you deal with breaches of compliance?
13. One of the principles of privacy entails justifying why the data is being collected by the department.
14. Since the principles have been adopted, has the City of Portland considered collecting data that they were previously not collecting?
15. Likewise, has any data been highlighted as data that is actually not necessary or not providing any additional value to the City's operations?
16. What have been some equity concerns that Portland has addressed or is in the process of resolving since the principles were adopted?
17. What were some of the actions that you had to take that you did not foresee coming prior to cities adoption of the principles?
Moving Forward

18. What to do still needs to be done - in terms of resources, awareness, practices etc. to ensure sustainable implementation of these principles?
19. What lessons can Oakland learn from Seattle and Portland?
Closing Request
Follow up via email if we need any feedback.

Appendix 2.C.

Expert	**Interview Date**	**Interview Type**	**Interviewers**
Deidre Scott	March 4, 2020	In-person at Oakland's City Clerk's Office	In-Person: Louis, Satoshi, Tony Phone Call: Randy
Hector Dominguez	April 24, 2020	Zoom	Jigyasa, Louis, Randy, Satoshi, Tony
Nancy Marcus	April 28, 2020	Phone Call	Randy, Tony
Kelsey Finch	April 29, 2020	Zoom	Jigyasa, Louis, Randy, Tony

Appendix 3

Below is a copy of the survey questions and the respective responses of each of the self-reported or identified departments and/or divisions.

Q.1 What kind of personal data does your division collect? (i.e. immigration status, social security, personal finances information) Please include the name of your department and/or division.	
City Department and/or Division	**Response**
City Clerk	Name, Address, Phone number
Unknown	Document title, Time and Date entered into the computer file only.
Unknown (possibly Contracts/Compliance)	(1) Combined Contract Schedules requires Federal ID# (2) Schedule E-2 (requires: 1) A valid photo ID is required to prove Oakland residency. Valid photo IDs include: a) U.S. Passport, b) Employment Authorization Document, c) State Driver's license or ID Card, d) School ID Card, and e) U.S. Military Card. 2) Other Acceptable Proofs of Oakland Residency: If the employee does not have a valid photo ID, the employer must submit at least two (2) other acceptable forms of proof of Oakland residency: a) Utility Bills, b) Bank Account Statements, c) Auto Registration, d) Mortgage Statements, e) Rental Agreements, and f) Verification of Public Assistance. 3) DE6 /DE9- Quarterly Wage and Withholding Report.)
Unknown	We visualize ID cards but do not copy; some documents that customers submit will have SSN, medical info, or personal finance info but are redacted.
City Administrator's Office	CAO - Special Activity Permits Social Security #, Financial Information (not regularly) Demographic (race, gender)- haven't started but will be soon
City Administrator's Office (Oak311 Call Center)	OAK311 collects your contact information related to one's request for Maintenance infrastructure service. My division is Oak311 Call Center, City Administrator's Office.
Finance (Parking Citations)	PCAC - personal finances, social security, health documents
Public Works (Contracts)	None. OPW/Contract Services
Finance (Revenue)	Personal finances information & social security. Finance Department, Revenue Division, Special Assessment Exemptions & Refunds
Finance (Business Tax)	Business income, social security - Business Tax Unit
Transport	None - Department of Transportation
Human Services Department, Aging & Adult Services Division	Human Services Department, Aging & Adult Services Division, Paratransit Program: Name, birthdate, address, phone, gender, race, emergency contacts, disability status and limited income data.
Human Services Department, Aging & Adult Services Division	HSD/Aging & Adult Services Division/ Senior Volunteer Services: Personal /client-Volunteer data. e.g. Socio-Econ data, Data is used to support Federal Grants. etc.

Q.2 Is the public informed on how data is ...?				
City Department and/or Division	**Collected**	**Used**	**Shared with Third Parties**	**Secured**
City Clerk	1	1	0	1
Unknown	0	0	0	0
Unknown (possibly Contracts/Compliance)	1	1	0	0
Unknown	1	1	0	1
City Administrator's Office	1	1	1	1
City Administrator's Office (Oak311 Call Center)	1	1	0	1
Finance (Parking Citations)	1	1	0	1
Public Works (Contracts)	0	0	0	0
Finance (Revenue)	1	1	0	0
Finance (Business Tax)	1	1	0	1
Transport	0	0	0	0
Human Services Department, Aging & Adult Services Division	1	1	0	1
Human Services Department, Aging & Adult Services Division	1	1	1	1

Q.3 What methods does your division use to collect data? Click all that apply								
City Department and/or Division	**Surveys**	**Website**	**Paper Forms**	**Surveillance Footage**	**In-Person**	**By Phone**	**Other**	**Please Specify**
City Clerk	1	1	1	0	0	0	0	
Unknown	0	0	1	0	0	0	0	
Unknown (possibly Contracts/Compliance)	0	0	1	0	0	0	0	
Unknown	0	0	1	0	1	0	0	
City Administrator's Office	0	0	1	0	0	0	0	
City Administrator's Office (Oak311 Call Center)	1	1	0	0	0	1	1	Emails and mobile app service requests.
Finance (Parking Citations)	0	1	1	0	1	1	0	
Public Works (Contracts)	0	0	1	0	0	0	0	
Finance (Revenue)	0	0	1	0	1	0	0	
Finance (Business Tax)	0	1	0	0	1	0	0	
Transport	0	0	0	0	0	0	0	
Human Services Department, Aging & Adult Services Division	0	1	1	0	0	0	0	
Human Services Department, Aging & Adult Services Division	1	0	1	0	1	0	1	Grant requirements to received Federal funds (e.g. Fingerprints)

Q.4 Why does your department collect personal data?	
City Department and/or Division	**Response**
City Clerk	Part of the business intake
Unknown	N/A
Unknown (possibly Contracts/Compliance)	Collected on behalf of City Administrator's office for contracting purposes.
Unknown	Payment plans; Appeals
City Administrator’s Office	Verification of Equity Status. Demographic Information needed to loan/grant program for reports on recipients
City Administrator’s Office (Oak311 Call Center)	OAK311 enters the contact information of the complainant.
Finance (Parking Citations)	Citizens are applying for fee waivers for hearing appearance, they are requesting dismissals of citations due to medical reasons
Public Works (Contracts)	N/A
Finance (Revenue)	To determine if homeowners qualify for Property Tax Special Assessment Refunds or Exemptions.
Finance (Business Tax)	To determine tax due and for collection purposes.
Transport	N/A
Human Services Department, Aging & Adult Services Division	Program/service eligibility purposes.
Human Services Department, Aging & Adult Services Division	Mandatory grant driven/programs require that all participants submit data documentation.

Q.5 How do you store personal data? Click all that apply						
City Department and/or Division	**Paper copies**	**USB, CD, or other portable storage devices**	**Employer-owned computers/devices**	**Third-Party drive (i.e. Google Drive, AWS, etc.)**	**Other**	**Please Specify**
City Clerk	1	0	0	1	0	
Unknown	1	1	1	1	0	
Unknown (possibly Contracts/Compliance)	1	0	0	0	1	Schedule E-2 is given to Contract Compliance. OPW Contract Services does not maintain copies.
Unknown	1	0	0	0	1	Redacted paper documents are scanned to Accela
City Administrator's Office	1	0	0	0	1	Shared drive
City Administrator's Office (Oak311 Call Center)	0	0	1	0	0	
Finance (Parking Citations)	1	0	1	0	0	
Public Works (Contracts)	0	0	0	0	0	
Finance (Revenue)	1	0	0	0	0	
Finance (Business Tax)	0	0	1	0	0	
Transport	0	0	0	0	0	
Human Services Department, Aging & Adult Services Division	1	0	1	0	0	
Human Services Department, Aging & Adult Services Division	1	1	1	0	1	Secured Files

Q.6 Do you...						
City Department and/or Division	**Share personal data with third parties?**	**Receive personal data from third parties?**	**Store personal data with third parties?**	**Sell personal data?**	**Sell personal data?**	**Sell personal data?**
City Clerk	0	0	0	0	0	
Unknown	0	0	0	0	0	
Unknown (possibly Contracts/Compliance)	0	0	0	0	0	
Unknown	0	0	1	0	0	Accela is a hosted offsite system - Might be considered 3rd party
City Administrator's Office	1	0	0	0	0	We share data collectively on the applicants, not on individuals
City Administrator's Office (Oak311 Call Center)	0	0	0	0	0	
Finance (Parking Citations)	0	0	0	0	0	
Public Works (Contracts)	0	0	0	0	0	
Finance (Revenue)	0	0	0	0	0	
Finance (Business Tax)	0	0	0	0	0	
Transport	0	0	0	0	0	
Human Services Department, Aging & Adult Services Division	0	0	0	0	0	
Human Services Department, Aging & Adult Services Division	1	1	0	0	0	

Q.7 Do you take any of the following data security measures?						
City Department and/or Division	**Encrypt**	**Backup**	**Anonymize**	**Restrict employee access to**	**Other**	**Please Specify**
City Clerk	1	1	0	0	0	
Unknown	0	1	1	0	0	
Unknown (possibly Contracts/Compliance)	0	0	0	1	0	
Unknown	1	0	0	0	1	Redact information - phone numbers; bank accounts; medical info; SSN, as per guidelines, etc.
City Administrator's Office	0	0	0	1	0	
City Administrator's Office (Oak311 Call Center)	0	1	0	0	0	
Finance (Parking Citations)	0	0	0	1	0	
Public Works (Contracts)	0	0	0	0	1	NA
Finance (Revenue)	0	0	0	1	1	Keep paper forms and copies of financial information on a secured floor.
Finance (Business Tax)	1	0	0	0	0	
Transport	0	0	0	0	1	N/A
Human Services Department, Aging & Adult Services Division	0	1	0	1	0	
Human Services Department, Aging & Adult Services Division	0	1	0	1	0	

Q.8 Do you request consent from individuals prior to ... their personal data?			
City Department and/or Division	**Collecting**	**Using**	**Sharing**
City Clerk	1	1	1
Unknown	1	1	1
Unknown (possibly Contracts/Compliance)	1	1	0
Unknown	0	1	0
City Administrator's Office	0	0	0
City Administrator's Office (Oak311 Call Center)	0	0	0
Finance (Parking Citations)	0	0	0
Public Works (Contracts)	0	0	0
Finance (Revenue)	1	1	0
Finance (Business Tax)	1	1	1
Transport	0	0	0
Human Services Department, Aging & Adult Services Division	1	1	1
Human Services Department, Aging & Adult Services Division	1	1	1

Q.9 Does your division inform the public of its data collection practices on its website/public forum?				
City Department and/or Division	**Yes**	**No**	**Other**	**Please Specify**
City Clerk	1	0	0	
Unknown	0	1	0	
Unknown (possibly Contracts/Compliance)	0	1	0	
Unknown	0	0	1	It is outlined in our fact sheets that are handed out per request
City Administrator's Office	0	1	0	
City Administrator's Office (Oak311 Call Center)	1	0	0	
Finance (Parking Citations)	0	1	0	
Public Works (Contracts)	0	1	0	
Finance (Revenue)	0	1	0	
Finance (Business Tax)	1	0	0	
Transport	0	0	1	N/A
Human Services Department, Aging & Adult Services Division	1	0	0	
Human Services Department, Aging & Adult Services Division	0	0	1	All program participants are notified that specific data is required to participate in the federally funded programs.

Q.10 Is there a designated staff member in your division who oversees personal data that is collected?				
City Department and/or Division	**Yes**	**No**	**Other**	**Please Specify**
City Clerk	1	0	0	
Unknown	0	1	0	
Unknown (possibly Contracts/Compliance)	0	0	1	Do not know
Unknown	0	1	0	
City Administrator's Office	0	1	0	
City Administrator's Office (Oak311 Call Center)	0	0	1	All OAK311 staff enter citizens contact information as part of their daily intake duties.
Finance (Parking Citations)	1	0	0	
Public Works (Contracts)	0	1	0	
Finance (Revenue)	0	1	0	
Finance (Business Tax)	0	1	0	
Transport	0	0	1	N/A
Human Services Department, Aging & Adult Services Division	1	0	0	
Human Services Department, Aging & Adult Services Division	1	0	0	

CITY OF OAKLAND

MEMORANDUM

TO: Privacy Advisory Commission

FROM: Roland Holmgren
Deputy Chief of Police

SUBJECT: OPD – FBI 2019 Joint Terrorism Taskforce (JTTF) Annual Report

DATE: May 20, 2020

EXECUTIVE SUMMARY

Ordinance No. 13457 C.M.S. approved by the City Council on October 3, 2017, adds Chapter 9.72.010 to the City of Oakland Municipal Code (OMC) concerning "Law Enforcement Surveillance Operations." OMC 9.72.010 requires that, among other requirements, that by January 31 of each year, the Chief of Police shall provide to the Privacy Advisory Commission (PAC) and City Council, a public report with appropriate public information on the Police Department's work with the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF) or other federal law enforcement agency task force in the prior calendar year.

STAFFING, EQUIPMENT AND FUNDING

As of January 1, 2019, one (1) employee (sworn OPD officer) was assigned to the FBI JTTF. The officer was assigned to work a standard regular work week of (40) forty hours per week. This officer is assigned to OPD's Intelligence Unit and has a joint duty of also participating and assisting with the FBI JTTF. The officer's duties and reporting responsibilities depend upon whether there is any active counter-terrorism investigation as well as the current needs and priorities of the OPD Intelligence Unit.

The position is compensated as a regular OPD officer; the FBI does not compensate OPD for this position's salary. The officer position works regular hours: 40 hours per week; 1,920 hours per year (approximately). Any overtime (OT) hours specific to taskforce operations are paid by the FBI - in 2019, the OPD JTTF Officer did not work any OT hours related to JTTF duties.

The JTTF-assigned officer was on special loan from the Intelligence Unit for most of 2019, assisting with upgrades to OPD's Bureau of Services Evidence Unit; the officer participated in monthly meetings with the JTTF during this time and actively assisted with investigations when requested. The upgrades to the OPD evidence unit are now complete enough that the officer can support both the OPD Intelligence Unit and JTTF information development (see ***Cases Assigned to the OPD JTTF Officer*** Section below), in addition to attending regular JTTF meetings.

OTHER RESOURCES PROVIDED

The FBI provided a vehicle, covered all fuel expenditures, and allowed access to the FBI JTTF office space and access to FBI data systems. OPD provides the mobile phone used by the Task Force (TF) Officer. The officer is not provided with any FBI surveillance equipment.

CASES ASSIGNED TO THE OPD JTTF OFFICER

The JTTF Officer assists the FBI on counter-terrorism cases. The OPD JTTF-assigned officer was assigned on special loan to OPD's Bureau of Services for the evidence unit for project support for most of 2019 as described above. Therefore, the officer was not assigned to any JTTF cases as a lead investigator; the JTTF Task Force Officer was assigned zero (0) cases as lead investigator in 2019. In 2019, there were five cases where the officer assisted the FBI as a secondary officer in a support role, primarily conducting research.

The following cases outline where the OPD JTTF-assigned officer assisted with investigations:

1. In February 2019, the FBI requested OPD assistance in identifying a location and suspect related to homicide threat. The OPD JTTF Officer utilized FBI information, assisted the FBI in eliminating several locations, helped connect individuals, and identified the exact location as well as the key suspect. This information allowed the FBI to issue a search warrant on the residence, and a suspect was arrested. The victim, a mother of two children, was unharmed and safely relocated with her children. The FBI, with the assistance of the JTTF Officer, very possibly saved a mother and her children from being murdered.
    - Suspect(s): One, Male Black
      Case Status: Open; Pending Trial
2. On June 25, 2019, the FBI notified the City of Alameda of a suspect, who had an active felony warrant for bomb threats to several east coast U.S. city police departments. The FBI believed there was a potential bomb threat to the City of Alameda based on the known information, so the JTTF Officer notified the Alameda Police Department. Separately, the suspect drove into the City of Oakland and was involved in a road rage incident in the 1400 block of Oak St. The suspect pursued the victim, who was riding on a motorcycle, and intentionally ran the motorcyclist over several times. The suspect was apprehended. The JTTF Officer responded to the crime scene and collaborated with outside agencies. No interviews were conducted by the JTTF Officer.
    - Suspect(s): One, Male White
    - Case Status: Open; Pending Trial

3. On June 27, 2019, suspects, armed with rifles, robbed a Loomis Armored Trunk in front of Wells Fargo in the City of Oakland, stealing approximately $500,000. The OPD JTTF Officer utilized OPD information to identify three suspects; Several search warrants were served, which led to the arrests of the suspects as well as significant evidence recovery.
    - Suspect(s): Three, Male Black
    - Case Status: Open; Pending Trial
4. Open investigation and will likely appear in 2020 report to PAC/City Council

5. Open investigation and will likely appear in 2020 report to PAC/City Council

The JTTF Officer participated in **zero (0) duty to warn cases**, where "Duty to Warn" is identified as the "requirement to warn U.S. and non - U.S persons of impending threats of intentional killing, serious bodily injury, or kidnapping".[1]

There were zero (0) cases in 2019 where OPD declined to participate after FBI request. The FBI knows that OPD task force officers must comply with all Oakland laws and policies. Furthermore, the FBI commonly works with different jurisdictions and understands that taskforces must collaborate with the particular polices and laws of those jurisdictions.

[1] FBI Duty to Warn – Intelligence Community Directive 191: https://fas.org/irp/dni/icd/icd-191.pdf

UNDERCOVER OPERATIONS AND INTERVIEWS

In 2019, the OPD JTTF Officer did **not participate in any joint FBI-OPD undercover operations or interviews** (JTTF interviews are normally conducted by FBI Agents); zero (0) undercover operations were conducted by the OPD JTTF-assigned officer. However, the officer did support informational gathering on behalf of JTTF investigations. The OPD officer only conducted information gathering, and did not work directly with FBI personnel on any actual operations.

In 2019, the OPD JTTF Officer did not take part in any interviews (voluntary or involuntary) - zero (0) were conducted.

In 2019, the OPD JTTF Officer did not conduct any assessments - zero (0) assessments conducted. Generally, unless someone were to come to the OPD to report a threat, all assessments begin with the FBI. Procedurally, FBI is notified, and an assessment is opened and FBI will then forward the assessment to specific agents.

The OPD JTTF Officer does not manage any informant relationships. In 2019, **there were zero (0) informant's managed by OPD JTTF Officer**. Furthermore, the Intelligence Unit Sergeant is the Informant Program Coordinator for all OPD informants. A file check was conducted on the JTTF Officer and there were zero (0) informant relationships related to the JTTF[2].

In 2019, there were no requests from outside agencies (e.g. Immigration and Customs Enforcement or "ICE") for records or data of OPD. There were no cases where the Task Force Officer was involved or aware of asking an individual's U.S. Person (residency) status. Furthermore, it is OPD Policy that OPD shall not inquire about a citizen's residency status.

The FBI is aware of requirements mandated of OPD and its protocols for undercover operations and interviews; the Task Force Officer was always held responsible for following all sworn officer policies and standards.

TRAINING AND COMPLIANCE

The OPD JTTF Officer follows all OPD policies and receives several police trainings, including but not limited to: continual professional training, procedural justice, and annual firearms training. The Officer has also reviewed all provisions of the JTTF MOU. The JTTF Officer as well as supervisor are held responsible by OPD for compliance with all applicable Oakland and California laws. The most recent list of trainings attended are as follows:

Date	**Training Type**
September 16, 2019	Criminal Investigations and Constitutional Law Update
September 17, 2019	Racial Profiling Update
September 18, 2019	Annual Firearms / Force Options Training
Ongoing	Virtual FBI training

[2] Identities of any informant would never be released to the public as such information is may be dangerous for the life of the informant.

The OPD JTTF Officer supervisor (Intel Sergeant) conducts mandatory bi-weekly meetings with the officer. Daily and weekly meetings are also held when critical incidents occur. Furthermore, the Intel Sergeant regularly works with the JTTF Officer in the same building/office located at the Police Administration Building (PAB). Additionally, the Sergeant supervising the officer in 2019 had U.S. Secret Service clearance and could review the work of the OPD JTTF Officer.

ACTUAL AND POTENTIAL VIOLATIONS OF LOCAL/STATE LAW

The JTTF OPD Officer had no violations of local, California, or Federal law. OPD Command consults with the Office of the City Attorney to ensure that all polices conform with State and Federal laws. Furthermore, a file check was conducted on the OPD JTTF Officer's complaint history in 2019 and there were zero (0) zero complaints against the Officer.

SUSPICIOUS ACTIVITY REPORTING (SARs) and NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER (NCRIC)

OPD submits Suspicious Activity Reports (SARs) to the Northern California Regional Intelligence Center (NCRIC). These reports contain information regarding activity, such as, but not limited to: narcotics, cyber-attacks, sabotage, terrorism threats, officer safety, and human trafficking. NCRIC provides a secure online portal where police agencies can provide this information. NCRIC has shared with OPD that providing false or misleading information to NCRIC is a violation of Federal Law and may be subject to prosecution under Title 18 USC 1001. The JTTF is a recipient of SAR information. The OPD JTTF Officer submitted zero (0) SARs to NCRIC during the 2019 calendar year. It is unknown how many SAR's OPD Officers received during 2019 as there is no current tracking system.

COMMAND STRUCTURE FOR OPD JTTF OFFICER

The OPD JTTF Officer works under the command structure of OPD; the OPD JTTF Officer reports directly to the OPD Intelligence Unit Supervisor (Sergeant). The Officer also coordinates with the FBI Supervisor, who is also serves as a Counterterrorism Assistant Agent.

Work in Progress

Oakland Privacy Advisory Commission Workplan 2020-21

Last update 6-24-20

Feb '20	Mar '20	Apr '20	May '20	Jun '20	Jul '20	Aug '20	Sep '20	Oct '20	Nov '20	Dec '20	Jan '21	Feb '21	Mar '21
	OPD Live Stream Camera Policy				OPD Forensic Logic Policy	OPD Automated License Plate Reader Policy	OPD FLIR Boat Policy	OPD ShotSpotter Annual Report	OPD Cellebrite Policy		OPD Hostage Throw Phone Policy	OPD Robot - Land Policy	OPD Cellsite Simulator Policy (conversion only)
					OPD JTTF Annual Report	OPD Body Worn Camera Policy	OPD Remote Camera Policy	OPD FLIR Helicopter Annual Report	OPD Starchaser Annual Report		OPD Live Stream Camera Annual Report	OPD Robot - Water Policy	
OPD Cell-site Simulator Annual Report		OPD Unmanned Aerial Device Policy				OPD FLIR Helicopter Policy (conversion only)	OPD Crime Lab Biometric Equipment Policy	OPD Pen-Link Policy				OPD Cell-Site Simulator Annual Report	
	PAC Annual Report		PAC Privacy Principles Update		PAC Agenda Management		PAC Privacy Principles Update				PAC Privacy Principles Update		PAC Annual Report
						DOT Automated License Plate Reader Annual Report	DOT Dockless Data Sharing Annual Report						
					City Mgr Sanctuary Contracting Annual Report								
		Chinatown Camera Grant Policy											

Department	Color
OPD	
DOT	
PAC	
OFD	
DPW	
City Manager/CPO	
IT	

Chapter 9.64 - REGULATIONS ON CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

Sections:

9.64.010 - Definitions.

The following definitions apply to this Chapter.

1. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:
   A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
   B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);
   C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
   D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year;
   E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall identify the race of each person that was subject to the technology's use.
   F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.
   G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
   H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
   I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
   J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year; and
   K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.
2. "Biometric Surveillance Technology" means any computer software that performs facial recognition or other remote biometric recognition in real time or on a recording or photograph.
3. "City" means any department, agency, bureau, and/or subordinate division of the City of Oakland as provided by Chapter 2.29 of the Oakland Municipal Code.
4~~3~~. "City Staff" means City personnel authorized by the City Administrator or designee to seek City Council approval of surveillance technology in conformance with this Chapter.

Formatted: Space After: 0 pt
Formatted: Font: 10 pt
Formatted: Font: (Default) Arial, 10 pt
Formatted: Font: 10 pt

5. "Continuing Agreement" means an agreement that automatically renews unless terminated by one (1) party.

65. "Exigent Circumstances" means a law enforcement agency's good faith belief that an emergency involving danger of, or imminent threat of the destruction of evidence regarding, death or serious physical injury to any person requires the use of surveillance technology or the information it provides.

76. "Face Recognition Technology" means (A) an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face; or (B) logs characteristics of an individual's face, head, or body to infer emotion, associations, expressions, or the location of an individual.

87. "Large-Scale Event" means an event attracting ten thousand (10,000) or more people with the potential to attract national media attention that provides a reasonable basis to anticipate that exigent circumstances may occur.

9. "Other Remote Biometric Recognition" means (A) an automated or semi-automated process that (i) assists in identifying an individual, capturing information about an individual, or otherwise generating or assisting in generating information about an individual based on the characteristics of the individual's gait or other immutable characteristic ascertained from a distance; (ii) uses voice recognition technology; or (iii) logs such characteristics to infer emotion, associations, activities, or the location of an individual, and (B) does not include identification based on fingerprints or palm prints.

108. "Personal Communication Device" means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable internet accessing devices, whether procured or subsidized by a city entity or personally owned, that is used in the regular course of city business.

11. "Predictive Policing Technology" means computer algorithms that use preexisting data to identify places or times that have a high risk of crime, or to identify individuals or groups who are likely to commit a crime.

129. "Police Area" refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

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

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

"Surveillance technology" does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined above:

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

B. Parking Ticket Devices (PTDs);

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

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

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

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

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

H. Police department interview room cameras.

I. Police department case management systems.

J. Police department early warning systems.

K. Personal communication devices that have not been modified beyond stock manufacturer capabilities in a manner described above.

1~~5~~2. "Surveillance Impact Report" means a publicly-released written report including at a minimum the following:

A. Description: information describing the surveillance technology and how it works, including product descriptions and manuals from manufacturers;

B. Purpose: information on the proposed purposes(s) for the surveillance technology;

C. Location: the location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);

D. Impact: an assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm;

E. Mitigations: identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;

F. Data Types and Sources: a list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom;

G. Data Security: information about the steps that will be taken to ensure that adequate security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure;

H. Fiscal Cost: the fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, the operative or proposed contract, and any current or potential sources of funding;

I. Third Party Dependence: whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;

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

K. Track Record: a summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).

16~~3~~. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

A. Purpose: the specific purpose(s) that the surveillance technology is intended to advance;

B. Authorized Use: the specific uses that are authorized, and the rules and processes required prior to such use;

C. Data Collection: the information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;

D. Data Access: the category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information;

E. Data Protection: the safeguards that protect information from unauthorized access, including encryption and access control mechanisms;

F. Data Retention: the time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;

G. Public Access: how collected information can be accessed or used by members of the public, including criminal defendants;

H. Third Party Data Sharing: if and how other city departments, 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;

I. Training: the training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology, and the identity or category of staff that will provide the training;

J. Auditing and Oversight: the mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and

K. Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

17. "Voice Recognition Technology" means the automated or semi-automated process that assists in identifying or verifying an individual based on the characteristics of an individual's voice.

Formatted: Indent: Left: 0.6", Hanging: 0.3"

Formatted: Indent: Left: 0.5", Hanging: 0.5"

(Ord. No. 13563, § 3, 9-17-2019; Ord. No. 13489, § 2, 5-15-2018)

9.64.020 - Privacy Advisory Commission (PAC) notification and review requirements.

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.

   A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:

      1. Seeking or soliciting funds for surveillance technology, including but not limited to applying for a grant; or,

      2. Soliciting proposals with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides.

   B. Upon notification by city staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, city staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action city staff will seek Council approval for pursuant to 9.64.030. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the city staff modify the proposal, or take no action.

   C. Should the Privacy Advisory Commission not make a recommendation pursuant to 9.64.020 1.B., City staff may proceed and seek Council approval of the proposed surveillance technology initiative pursuant to the requirements of Section 9.64.030.

2. PAC Review Required for New Surveillance Technology Before City Council Approval.

   A. Prior to seeking City Council approval under Section 9.64.030, city staff shall submit a surveillance impact report and a surveillance use policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

   B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed surveillance use policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to city staff. City staff shall present such modifications to City Council when seeking City Council approval under Section 9.64.030.

   C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval.

   A. Prior to seeking City Council approval for existing city surveillance technology under Section 9.64.030 city staff shall submit a surveillance impact report and surveillance use policy to the Privacy Advisory Commission for its review at a regularly noticed meeting. The surveillance impact report and surveillance use policy must address the specific subject matter specified for such reports as defined under 9.64.010.

   B. Prior to submitting the surveillance impact report and proposed surveillance use policy as described above, city staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the city.

   C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.

   D. Within sixty (60) days of the Privacy Advisory Commission's action in 9.64.020 1.C., city staff shall submit at least one (1) surveillance impact report and proposed surveillance use policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a policy has been submitted for each item on the list.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within ninety (90) days of submission shall enable city staff to proceed to the City Council for approval of the item pursuant to Section 9.64.030.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.030. - City Council approval requirements for new and existing surveillance technology.

1. City staff must obtain City Council approval prior to any of the following:
   A. Accepting state or federal funds or in-kind or other donations for surveillance technology;
   B. Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;
   C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner, or in a location not previously approved by the City Council pursuant to the requirements of this Chapter; or
   D. Entering into a continuing agreement or written agreement with a non-city entity to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.
   E. Notwithstanding any other provision of this Section, nothing herein shall be construed to prevent, restrict or interfere with any person providing evidence or information derived from surveillance technology to a law enforcement agency for the purposes of conducting a criminal investigation or the law enforcement agency from receiving such evidence or information.
2. City Council Approval Process.
   A. After the PAC notification and review requirements in Section 9.64.020 have been met, city staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed surveillance impact report and proposed surveillance use policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing.
   B. The City Council shall only approve any action as provided in this Article after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.
   C. For approval of existing surveillance technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under 9.64.020 3.E, if the City Council has not reviewed and approved such item within four (4) City Council meetings from when the item was initially scheduled for City Council consideration, the city shall cease its use of the surveillance technology until such review and approval occurs.
3. Surveillance Impact Reports and Surveillance Use Policies are Public Records. City staff shall make the Surveillance Impact Report and Surveillance Use Policy, as updated from time to time, available to the public as long as the city uses the surveillance technology in accordance with its request pursuant to Section 9.64.020 A.1.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.035 - Use of unapproved technology during exigent circumstances or large-scale event.

1. City staff may temporarily acquire or use surveillance technology and the data derived from that use in a manner not expressly allowed by a surveillance use policy in two (2) types of circumstances without following the provisions of Section 9.64.030: (A) exigent circumstances, and (B) a large-scale event.
2. If city staff acquires or uses a surveillance technology in the two (2) circumstances pursuant to subdivision 1., the city staff shall:
   A. Use the surveillance technology to solely respond to the exigent circumstances or large-scale event.
   B. Cease using the surveillance technology when the exigent circumstances or large scale event ends.
   C. Only keep and maintain data related to the exigent circumstances and dispose of any data that is not relevant to an ongoing investigation.
   D. Following the end of the exigent circumstances or large-scale event, report that acquisition or use to the PAC at their next respective meetings for discussion and/or possible recommendation to the City Council in accordance with the Sunshine Ordinance, the Brown Act, and City Administrator deadlines.
3. Any technology temporarily acquired in exigent circumstances or during a large-scale event shall be returned within seven (7) days following its acquisition, or when the exigent circumstances end, whichever is sooner, unless the technology is submitted to the City Council for approval pursuant to Section 9.64.030 and is approved. If the agency is unable to comply with the seven-day timeline, the agency shall notify the City Council, who may grant an extension.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.040 - Oversight following City Council approval.

1. ~~On March 15th of each year~~, ~~or at the next closest regularly scheduled Privacy Advisory Commission meeting~~For each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission review ~~for each approved surveillance technology item~~a year from the date that the corresponding use policy was approved by the City Council, and annually thereafter as long as the technology is in use. If city staff is unable to meet the ~~March 15th~~ deadline, city staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.
   A. After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council.
   B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the corresponding surveillance use policy that will resolve the concerns.
   C. Failure by the Privacy Advisory Commission to make its recommendation on the item within ninety (90) days of submission shall enable the city entity to proceed to the City Council for approval of the annual surveillance report.
   D. ~~In addition to the above submission of any Annual Surveillance Report, city staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to Section 9.64.030 and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed surveillance use policy before approval.~~

2. Based upon information provided in city staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in Section 9.64.030 2.B. and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the city's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.045 - Prohibition on City's acquisition and/or use of (i) ~~face recognition technology~~biometric surveillance technology, or (ii) predictive policing technology~~.~~

A. Notwithstanding any other provision of this Chapter (9.64), it shall be unlawful for the City or any City staff to obtain, retain, request, access, or use:

1. ~~Face recognition technology~~Biometric surveillance technology; or

2. Predictive policing technology; or

3~~2~~. Information obtained from either ~~face recognition~~biometric surveillance technology or predictive policing technology.

B. City staff's inadvertent or unintentional receipt, access of, or use of any information obtained from ~~face recognition~~biometric surveillance technology or predictive policing technology shall not be a violation of this Section 9.64.045 provided that:

1. City staff did not request or solicit the receipt, access of, or use of such information; and

2. City staff shall immediately destroy all copies of the information upon its discovery and shall not use the information for any purpose; and

3~~2~~. City staff logs such receipt, access, or use in ~~its annual surveillance report as referenced by Section 9.64.040~~a written report provided at the next closest regularly scheduled meeting after discovery of the use, to the Privacy Advisory Commission for discussion and possible recommendation to the City Council. Such report shall not include any personally identifiable information or other information the release of which is prohibited by law. In its report, City staff shall identify specific measures taken by the City to prevent the further transmission or use of any information inadvertently or unintentionally obtained through the use of such technologies; and

4. After review by the Privacy Advisory Commission, city staff shall submit the report to the City Council.

(Ord. No. 13563, § 3, 9-17-2019)

9.64.050 - Enforcement.

1. Violations of this Article are subject to the following remedies:

A. Any violation of this Article, or of a surveillance use policy promulgated under this Article, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Article. An action instituted under this paragraph shall be brought against the respective city department, and the City of Oakland, and, if necessary to effectuate compliance with this Article or a surveillance use policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Article, to the extent permitted by law.

Formatted: Indent: Left: 0.3", First line: 0"

B. Any person who has been subjected to a surveillance technology in violation of this Article, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Article or of a surveillance use policy promulgated under this Article, may institute proceedings in the Superior Court of the State of California against the City of Oakland and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).

C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraphs A. or B.

D. Violations of this Article by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.060 - Secrecy of surveillance technology.

It shall be unlawful for the city to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Article, and any conflicting provisions in such future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable.

To the extent permitted by law, the city shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

(Ord. No. 13489, § 2, 5-15-2018)

9.64.070 - Whistleblower protections.

1. Neither the city nor anyone acting on behalf of the city may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms and conditions of employment, access to information, restrictions on due process rights, or civil or criminal liability, because:
   A. The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Article; or
   B. The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Article.
2. It shall be grounds for disciplinary action for a city employee or anyone else acting on behalf of the city to retaliate against another city employee or applicant who makes a good-faith complaint that there has been a failure to comply with any surveillance use policy or administrative instruction promulgated under this Article.
3. Any employee or applicant who is injured by a violation of this Section may institute a proceeding for monetary damages and injunctive relief against the city in any court of competent jurisdiction.

(Ord. No. 13489, § 2, 5-15-2018)

OAKLAND POLICE DEPARTMENT

Surveillance Impact Report:

Forensic Logic, Inc. CopLink Search and Crime Report System

A. Description: Crime Analysis Report System and CopLink Search, and How they Work

The Forensic Logic, Inc. ("Forensic Logic") supported crime analysis report system is based on a comprehensive categorization and organization of California penal code offense types that allows OPD crime analysts to produce various crime reports such as point in time, year-to-date and year-to-year comparisons. The categorization takes thousands of penal code types and organizes the data into several hierarchies in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) Uniform Crime Reporting (UCR) Part One and Part Two crimes.

The CopLink search engine combines criminal justice information from various law enforcement systems owned and operated by agencies throughout the United States. Forensic Logic maintains a secure data warehouse within the Microsoft Azure Government Cloud. Core datasets include computer-aided dispatch (CAD) and record management system (RMS) crime incident data (see "Elements of the Search" on "Data Types and Sources Section – pages 14,15 below for list of features).

Forensic Logic first built their data warehouse by focusing on search engine technology; they built indexing algorithms to understand natural language, decode law enforcement vernacular, extract entities and relationships from the data, and then rank results based on the seriousness of the offense and the proximity to a user's location and time of event.. The original LEAP search system allowed for the aggregation of structured, semi-structured and unstructured data into a common repository.

International Business Machines (IBM) originally acquired CopLink in 2012; Forensic Logic has since purchased CopLink from IBM and begun to integrate the two systems under the brand of Forensic Logic CopLink.

Crimes committed in Oakland are sometimes connected to crimes, suspects, and evidence from crimes in neighboring cities. The Forensic Logic CopLink system integrates data that may come from outside agencies but that relates to crime that occurs in Oakland. Additionally,

providing OPD data to other agencies in the region empowers those agencies to better investigate crimes that have a nexus to Oakland.

Forensic Logic CopLink takes the diverse data sources and types and uses algorithms to rank searches based on a hierarchical weighted logic system. For example, data connected to more serious and violent crime is ranked higher; data related to more geographically close data is ranked higher; and more recent data is ranked higher.

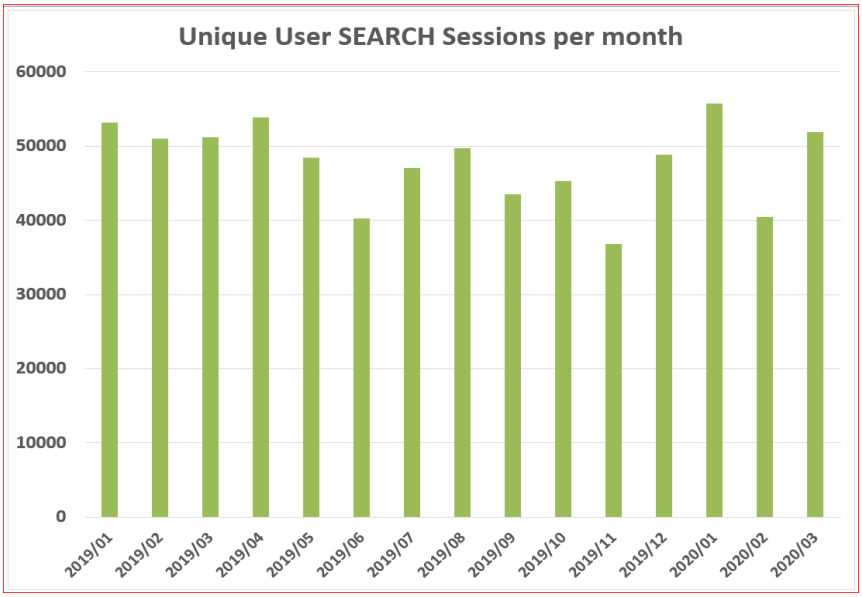
B. Proposed Purpose

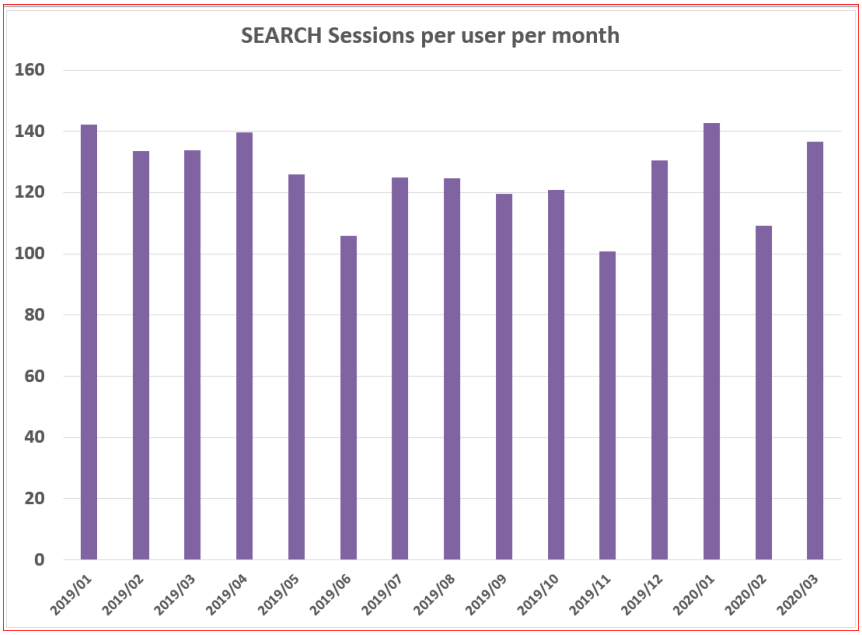
Forensic Logic provides three core services for OPD: a) crime analysis report production; b) search; and c) technical assistance**.**

1. Crime Analysis Report Production – Forensic Logic has built a comprehensive categorization and data organization structure that allows OPD crime analysts to better access OPD's own data - the categorization takes thousands of penal code types and organizes the data in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) UCR Part One and Part Two crimes.

   These reports provide useful information about crime trends in easily consumable formats (year-to-date, point in time, and year-to-year comparisons). The reports summarize key crime types such as robberies and burglaries, summarizing hundreds of sub-penal codes. The reports are also sub-divided into each of the five police areas. These reports are regularly used by both the Office of the Mayor and City Council as well as members of the public. These reports are also used by Community Resource Officers (CROs) to present crime updates to Neighborhood Crime Prevention Councils (NCPCs) throughout the City. The technology allows for a streamlined process that would take orders of magnitude in additional staff hours were crime analysts to compile the reports using only OPD-owned technology.

2. Search – Officers and other assigned personnel need access to well organized law enforcement data to solve serious and violent crime, such as homicides and robberies. The following tables provide data on actual OPD Forensic Logic CopLink search usage (unique searches by month, number of searches per officer per month).


Unique User SEARCH Sessions per month
60000
50000
40000
30000
20000
10000
0
2019/01
2019/02
2019/03
2019/04
2019/05
2019/06
2019/07
2019/08
2019/09
2019/10
2019/11
2019/12
2020/01
2020/02
2020/03


SEARCH Sessions per user per month
160
140
120
100
80
60
40
20
0
2019/01
2019/02
2019/03
2019/04
2019/05
2019/06
2019/07
2019/08
2019/09
2019/10
2019/11
2019/12
2020/01
2020/02
2020/03

CopLink: Critical Tool for Crime Investigations

Criminal Investigation Division (CID) investigators use the Forensic Logic CopLink search capability (formerly known as LEAP) daily and run the majority of their cases through the search portal to look for suspects or any leads. The following examples highlight some of the many ways LEAP / CopLink is used many times every day by CID investigators, patrol officers, and officers assigned to special units:

- An officer assigned to OPD's Ceasefire Strategy[1] was provided a nickname for a shooting suspect, but was not provided any further identifying information. The officer conducted a query of the nickname in CopLink and due to the uniqueness of the nickname was able to determine her identity from a human-trafficking investigation. The nickname apparently was the alias that she used during that arrest. The officer conducted additional queries using the suspect's true name and found numerous contacts between her and the primary shooting suspect. The large majority of these contacts were from the Las Vegas, NV metro area, and this provided an important new source of information**.**

- There was a shooting in January 2020 in West Oakland. A typo caused an incorrect telephone number to be entered into OPD's CAD. The investigator was nonetheless able to find additional contact information for the witness in CopLink using different variations of the witness' name; this search led to a good telephone number from a report she had filed the previous year. The officer called this witness and she provided useful information which led to a charge in the case.

- A CID investigator was able to identify a suspect using CopLink in a serious sexual assault case and connect the suspect to two additional reports where he is listed as suspect of similar sexual assaults – San Leandro PD and Hayward PD were also able to connect the same suspect to their cases using CopLink.

- An officer who was investigating a violence against woman crime[2] found a suspect who was also linked to a similar prior crime; the officer was able to connect with this previous victim, obtain testimony and provide a level of support and justice that so far had not occurred. The OPD officer was able to combine data from the cases to further the investigation of each case.

- A homicide investigator was able to recently connect a nickname

[1] https://www.oaklandca.gov/topics/oaklands-ceasefire-strategy
[2] https://www.justice.gov/ovw/about-office

to a legal name of a suspect of in a recent homicide, now charged by the District Attorney's Office; this officer confirms using LEAP / CopLink on almost every homicide investigation over several years.

- A CopLink search revealed the suspect vehicle involved in a recent East Oakland robbery was also involved in one in City of San Francisco. The investigator collaborated with the San Francisco Police Department (SFPD) and ultimately wrote an arrest warrant.

- A CopLink search on an auto burglary suspect vehicle, revealed that the suspect vehicle was connected to several other auto burglaries. Officers located and towed the suspect vehicle. The vehicle is now being analyzed by OPD evidence technicians for more clues.

- A firearm assault and shooting case resulted in an arrest and charge, as video footage showed a unique SUV; officers used CopLink to search for the SUV using descriptive terms, which led to an address and search warrant.

The CopLink platform facilitates the revelation of information vital to the expeditious and successful conclusion of criminal investigations in two ways: (i) through the collection of many types of structured and unstructured (e.g. text narratives) law enforcement data originating from many different law enforcement agencies; and (ii) the continuous ranking of the data as it enters the CopLink platform based on a number of factors including seriousness of offense, proximity to a user's search location and recency of the data so a user conducting a search finds the information being sought in the first pages of the resulting list of documents.

As is often the case, offenders are mobile and have had encounters with law enforcement in many jurisdictions and the collection of data from multiple law enforcement agencies in the CopLink platform provides broader coverage for the search engine to locate related information.

3. Technical Assistance

   OPD occasionally solicits Forensic Logic's technical expertise to integrate and tabulate data such as from OPD Field Based Reporting systems to analyze stop data. Forensic Logic has also assisted OPD with the following projects over the past few years:

   a. The development of the first OPD CompStat weekly review using both interactive Google Earth maps and detailed Area maps and reports;

b. The development of the first Stop Data search and analysis system employed by the Federal Independent Monitoring Team and used successfully by OPD to achieve many of the criteria required of Task 34 of the NSA; staff from the OPD Office of the Inspector General still use CopLink for risk management assessments.
c. The evaluation and analysis of OPD's reporting to the FBI of monthly UCR reports to confirm that incidents were reported correctly and in a timely manner; and
d. The facilitation of the Forensic Logic search roduct for use on OPD mobile devices in the field.

C. Locations Where, and Situations in which the Forensic CopLink System may be deployed or utilized.

The technology is provided to patrol officers, investigators, and other appropriate personnel. The system is also used within the Department primarily by crime analysts to produce weekly and customized crime reports that are used by the Mayor's Office and the City Council. The Weekly Crime Report (April 20-26, 2020) (see ***Appendix A*** at end of this report) was produced by the OPD Crime Analysis Unit with the assistance of Forensic Logic and their offense categorization developed to compile the report. The report provides data on Type 1 crimes occurring in Oakland during the week of April 20-26, 2020 with comparisons to the year to date 2018, 2019, and 2020.

D. Impact

The aggregation of data will always cause concern of impacts to public privacy. Data collected and stored in the Forensic Logic CopLink network has previously been collected by law enforcement agencies in an originating data source. Those data sources include calls for service (originated in Computer Aided Dispatch systems); incident reports, field contacts and arrests (originated in Records Management Systems); time and location where firearms have been discharged (originated from from Gunshot Location Systems); time, location, description and disposition of on-view field contacts; warrants and wants from probation, parole and court systems; booking information and mug shots (originated from Jail Management Systems); and description of events reported by the public compiled in drug hotline and other tip lines. Data is already collected, stored and shareable with other law enforcement agencies by OPD.

Oakland residents who may not have a legal immigration status have a right to privacy. The California Values Act (SB 54 [3]) is enacted to ensure that (barring exceptions contained in the law), no state and local resources are used to

[3] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB54

assist federal immigration enforcement. Forensic Logic has developed protocols described below in the mitigations section which mitigate the potential for the release of data which could impact immigration status-related privacy rights.

OPD understands that members of the Oakland community as well as the Privacy Advisory Commission (PAC) are concerned about potential privacy impacts associated with OPD's use of ALPR. For this reason, for the past five years OPD has not allowed its ALPR data to be entered into Forensic LEAP Search or Forensic Logic CopLink system and all prior collected ALPR data has been expunged from the system – even though many other participating agencies share ALPR data, and OPD could benefit from this data commingled in the Forensic Logic CopLink system.

Forensic Logic complies with all federal (e.g. FBI CJIS Security Addendum), state (e.g. SB 54) and local laws (e.g. Oakland Sanctuary City Ordinance[4]) ~~and ordinances~~ associated with use of collected law enforcement data. This includes, in the state of California and many individual jurisdictions, the prohibition on the use of facial recognition and the analysis of body worn camera video data.

E. Mitigations

OPD and Forensic Logic utilize several strategies to mitigate against the potential for system abuse and/or data breach.

System Mitigations

In accordance with CJIS Security Policy (CSP) 5.8[5], the Forensic Logic CopLink application keeps all user access and activity logs, which can be made available to agency command staff and/or administrators at any time – OPD has the ability to request detailed query logs of OPD personnel CopLink usage. Per FBI CJIS Security Policy v5.8, Paragraph 5.4, Forensic Logic logs information about the following events and content and a report can be produced upon request at any time:

5.4.1.1 Events

The following events shall be logged:

1. *Successful and unsuccessful system log-on attempts.*
2. *Successful and unsuccessful attempts to use:*
    a. access permission on a user account, file, directory or other system resource;

[4] https://oakland.legistar.com/LegislationDetail.aspx?ID=3701155&GUID=8153C1B0-B9FC-4B29-BDDE-DF604DEDAEAD&Options=&Search=

[5] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

b. create permission on a user account, file, directory or other system resource;
c. write permission on a user account, file, directory or other system resource;
d. delete permission on a user account, file, directory or other system resource;
e. change permission on a user account, file, directory or other system resource.

3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
a. access the audit log file;
b. modify the audit log file;
c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware
component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

Therefore, OPD has the ability to conduct audits if there is reason to believe the system is not being used in accordance with criminal investigation protocols.

Data Security Mitigations

Section G below (Data Security) provides an in-depth explanation of the many ways the Forensic Logic CopLink system itself is secure to data breaches. Data that is deleted from OPD CAD/RMS or other systems is automatically deleted from the Forensic Logic CopLink system.

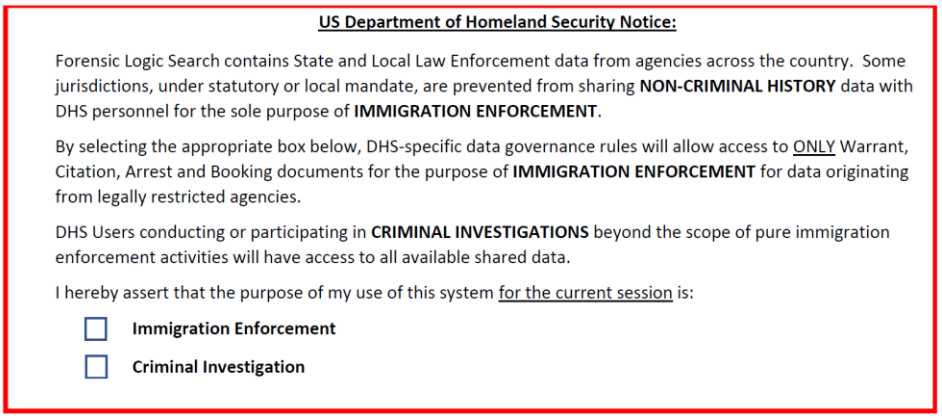
Safeguards in Alignment with Oakland and California Immigrant Legal Protections

Forensic Logic has created technical mitigations to ensure that cities in California and elsewhere can use Forensic Logic CopLink while complying with SB54 and similar sanctuary city laws. Forensic Logic allows participating agencies to elect how their agency-generated data is shared within the Forensic Logic CopLink system.

Firstly, agencies such as OPD can specify that no data be shared with select federal law enforcement users – regardless of whether the query is for immigration-specific purposes. OPD has specified (current and future contracts)

this protocol for sharing data so that no OPD data is shared with ICE or its Homeland Security Investigations (HSI) section

Forensic Logic partners with several federal agencies: The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the FBI, and the U.S. Marshals Service (two of the 94 U.S. Attorney Districts). Forensic Logic did have one contract with Immigrations, Customs and Enforcement (ICE) that expired on May 15, 2020. However, Forensic Logic is not seeking to further contract with ICE or other agencies prohibited from Oakland partnership under OMC 2.23.030. This contract, in fact, was created to examine how Forensic Logic could best isolate police agency data from any Department of Homeland Security (DHS)[6] searches. Some police departments (such as Oakland) want to ensure that ICE never has access to their data, while there are also agencies that only want ICE's HSI Section to have access for purely criminal (non-immigration) type investigations. Forensic Logic CopLink has since developed the following logic model in these cases for Department of Homeland Security queries:



This system does not apply to Oakland since Oakland data is never available to any DHS agencies – or to other federal agencies OPD may in the future specify.

Limited Access Mitigations

OPD strives to balance the use of surveillance technology and support of public privacy. The "Impact" section above explains that OPD disallows its ALPR data to be shared with any other agency that subscribes to Forensic Logic CopLink.

OPD has additionally requested that OPD personnel not have access to the following CopLink features: 1) HotBlocks; and 2) *Next Crime Location*.

The Hotblocks" feature in CopLink Analytics illustrates incident clusters (see ***Appendix B*** for illustration). This feature is a geospatial tool for plotting ~~similar~~

[6] ICE is one of several agencies organized within the umbrella DHS agency.

incidents in close proximity to each other on a map ~~given incident locations~~. The 'math' looks at latitude/longitude - and then calculates how near some dots on the map are to all other dots on the map. It is used as a tool to investigate location-specific crimes such as burglary, arson and auto theft/auto recovery. Investigators can use the visualization – along with other data and evidence to help identify leads. This type of work is integral to intelligence-led policing. However, OPD has requested that Forensic Logic remove this analytical tool from OPD CopLink access because the Privacy Advisory Commission expressed concern at the June 4, 2020 meeting that this tool could represent a form of "predictive policing." OPD and Forensic Logic ~~see~~concur that this tool does not actually make predictions, but rather helps personnel with their analysis of where crimes are occurring. However, OPD will not use this module out of respect to concerns that this tool is perceived to impact public privacy.

The Next Crime Location (NCL) (see ***Appendix C*** for illustration) is similar to HotBlocks in that it also displays on a map the relationship of incident locations (X-Y grid) and their relationship to the center of mass of those X-Y points and one, two and three standard deviation distribution from that center of mass. NCL takes geographic incident data and calculates mathematical spaces around the center of gravity of the dot. OPD and Forensic Logic ~~see~~concur that this tool does not actually make predictions, but rather helps personnel with their analysis of where location-based crimes such as arson, burglary and auto theft/auto recovery are occurring (as with the HotBlocks feature), OPD will not use this module out of respect to the PAC's expressed concerns that this tool is perceived to negatively impact public privacy.

Data Access Safeguards

Indexing of public data into CopLink provides another tool that balances function and privacy mitigations. Some agencies subscribe to public data databases such as Thomson Reuters CLEAR (TRC). The Forensic Logic CopLink network has indexed abstracts (summary information lacking details) of certain public records available in the TRC service so that a single search in the Forensic Logic CopLink search service will reveal that the TRC service has more information about the topic. The data itself is not actually in CopLink – just an index of data type (similar to a library card catalog), similar to how common search engines index data without actually containing the data. Therefore, OPD cannot access this type of data (since OPD does not subscribe to TRC) - and the CopLink system queries will not show that more information is available in TRC.

OPD data additionally cannot be accessed by ICE nor other non-authorized agencies via the National Law Enforcement Telecommunications System (NLETS)[7]. NLETS is the main interstate justice and public safety network in the nation for the exchange of law enforcement, criminal justice, and public safety-related information. NLETS is a private, not--for--profit corporation owned by all

[7] https://www.nlets.org

50 U.S. states; the user population is made up of all of the United States and its territories, all Federal agencies with a justice component, selected international agencies, and a variety of strategic partners that serve the law enforcement community-cooperatively exchanging data. NLETS provides two basic functions:

1. A communication network that switches queries primarily from law enforcement officers to law enforcement sensitive data stored at state Departments of Motor Vehicles (DMV) and the FBI National Crime Information Center (NCIC) where among other data sets, data about stolen vehicles and felony warrants is collected; and
2. A co-location and virtual data center where vendors associated with law enforcement (e.g. Forensic Logic) can rent space, power and virtual machines (computer servers) in a CJIS protected physical environment.

For the most part, NLETS does not store or collect data (only the message queries from its users and message responses), but rather transmits data directly to authorized users over its network from data owners such as the DMV and NCIC where stolen vehicle and felony warrant data is centralized. OPD incident data is not stored in NLETS; therefore, neither ICE nor other agencies can utilize CopLink and NLETS to access OPD data.

F. Data Types and Sources

Forensic Logic has created file transfer protocol data feeds to automatically ingest several data systems into the CopLink system. These data include CAD/RMS, field-based reporting module data, calls for service, and ShotSpotter data that could be used to populate an ATF eTrace[8] gun tracing form. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system.

An exhaustive list of data sets ingested by Forensic Logic CopLink from OPD data sources follows.

Data Source Collected	Collection Status	Retention Policy	Access Conditions
Arrest	Active	Perpetual	Only law enforcement; US DHS prohibited
Field Contacts	Active	Perpetual	Only law enforcement; US DHS prohibited

[8] https://www.atf.gov/resource-center/fact-sheet/fact-sheet-etrace-internet-based-firearms-tracing-and-analysis

Incident Reports	Active	Perpetual	Only law enforcement; US DHS prohibited
Calls for Service	Active	Perpetual	Only law enforcement; US DHS prohibited
Stop Data	Active	Perpetual	Only law enforcement; US DHS prohibited
Traffic Accident	Active	Perpetual	Only law enforcement; US DHS prohibited
ShotSpotter	Active	Perpetual	Only law enforcement; US DHS prohibited
ATF NIBIN Ballistics	Proposed	Perpetual	Only law enforcement; US DHS prohibited

The purpose of the Forensic Logic CopLink network is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. This information assists authorized agencies in criminal justice and related law enforcement objectives, such as apprehending subjects, locating missing persons, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system (see ***Appendix D*** below for a list of all agencies that are clients of Forensic Logic and have access to OPD data through CopLink Search[9]).

There are many types of OPD data that, by policy and process, will not be sent to Forensic Logic CopLink or to other Forensic Logic CopLink client agencies. The following data types and sources are not sent to Forensic Logic:

- OPD ALPR data
- Data from other City of Oakland Departments (e.g., code compliance data from Planning and Zoning).
- Unverified data from ongoing investigations
- Intelligence briefings
- Body worn camera video

[9] This list represents all agencies who are able to see OPD data. These agencies do not actually necessarily see OPD data; OPD data only comes up in a search result list if something in the record has the same terms as those that a user puts into the search box. The further away from the location of the incident, an OPD record is unlikely to be in the top few results pages unless the exact person is found.

- Data that includes the identities of confidential informants
- Any data that is categorized as criminal intelligence subject to 28 CFR Part 23 analysis or processing of booking or other photos for the purposes of identification of the subject using facial recognition[10] capabilities

There are three services that Forensic Logic provides to OPD: 1) Analytics for Crime Reports; 2) Search; and 3) technical assistance.

Forensic Logic provides its Search services as an enterprise subscription available to all sworn officers and authorized professional staff operating under the auspices of the Chief of Police.

The Forensic Logic CopLink enterprise service is broken down into a number of components. The two primary components (used by OPD) are: 1) Analytics; and 2) Search.

There are several elements to the Analysis component – all of which are specialized presentations of the analysis capability within the Forensic Logic CopLink network:

- There is a more structured search capability than exists in the Search product that allows users to specify the parameters for each structured field in a report. An additional capability permits the structured search to be saved and directed to constantly monitor new data as it enters the system so that users are notified when the search terms satisfy new data. For example, if one is seeking a vehicle with a particular vehicle tag, they can create that search and request that any time that same vehicular tag is mentioned in a future report that I am to be notified.
- There is a reporting module that flexibly allows users to structure reports based on offense categories, time frames and geographical areas.
- There is a mapping component that allows one to visualize records in a particular region based on a number of structured data in a large number of data fields
- The geonet capability places linked incidents on a map so that both geospatial characteristics and common linked characteristics of crimes can be visualized
- The timeline feature organizes linked incidents by ordering the incidents chronologically and displaying those incidents on a map with connector lines illustrating the chronological timeline of the events

[10] Forensic Logic Product Modules (see ***Appendix B***) shows that the older "Legacy" previously owned by IBM offered a feature called "FaceMatch" facial recognition. This system was used to provide five other faces similar to a suspect photo so victims and witnesses can look at the "6-pack" of faces and attempt to identify a person or suspect, similar to a line-up. Face-match is not in OPD's LEAP – rebranded as CopLink and Forensic Logic is not incorporating this technology into the new CopLink.

All of the analytics modules above are included with the subscription to the CopLink Analytics service in the Forensic Logic CopLink network and are not provided independently. OPD has successfully negotiated an enterprise subscription to the Forensic Logic CopLink Analytics product at no additional charge so all OPD sworn officers and authorized professional staff under the auspices of the Chief of Police will have access to all Analytics capabilities at no additional fee.

There are several "Elements of the Search" component – all of which are specialized presentations of search:

- The search bar operates exactly as a user would expect a google search to operate with the one exception being the ranking of results is optimized for law enforcement rather than advertising (as is the focus of a Google search since advertisers financially support the operation of the Google search capability).
- The Tag Cloud element is another presentation of how search results are visualized by increasing the font size in a Tag Cloud to be representative of the number of occurrences that a particular phrase occurs in the Forensic Logic CopLink system or a subset of the data.
- The Facet search is a tool that organizes search capabilities into a number of static categories such as offense descriptions, agencies, document types and vehicle tags, amongst other categories.
- The time search capability permits users to quickly drill down to specific years, months, days or times of incidents with simple button selections.
- Timeline search organizes the same data visually on a timeline so incidents and calls for service in subsets resulting from a ~~g~~Google-like search can be organized chronologically.
- Geospatial search permits a user to select geographies such as Beats or Areas; areas around schools; or custom areas selected using the user's mouse to draw areas on a map in order to visualize and select incident reports associated with the specific geographic region.
- The search Charting module organizes search results into categories visualized by bar charts such as offense descriptions, time of day, day of week, vehicle model and agency Beat amongst other data fields.
- The link chart capability produces a visualization of records that are linked based on a number of criteria including name, offense and location.

All of the search modules above are included with the enterprise subscription to the CopLink SEARCH service in the Forensic Logic CopLink network and are not provided independently

Forensic Logic provides its Analytics services as a Named User subscription available to selected sworn staff and authorized professional staff operating under the auspices of the Chief of Police.

Forensic Logic CopLink can also consists of the following modules: CopLink Connect (formerly called forums); CopLink Dashboard, and CopLink Trace. (gun-tracing). CopLink Connect is a secure internal communication system for intra-agency CJIS-compliant communications. OPD does use this system to securely share investigations information internally between personnel – no information is shared with any agency outside of OPD. Alternatives to this system are email or non-CJIS-compliant systems (e.g. box.com).

OPD utilized CopLink Dashboard in the past (see "Proposed Purpose" Section above as well continued here in "Data Types and Sources" below) for use with stop data analysis. OPD now uses other non-Forensic Logic systems for stop data analysis and does not use CopLink Dashboard; OPD does not have access to the Dashboard module.

CopLink Trace is a system used for gun-tracing; OPD does not have access to this module and does not utilize this module.

OPD occasionally calls upon Forensic Logic for technical assistance, to collaborate on tasks where data can be used to solve a particular problem. An example of projects that Forensic Logic has undertaken for OPD where Forensic Logic did not charge additional fees include:

- Development of weekly CompStat reporting and presentation system displayed on google Earth illustrating location of major offenses on a map as well as all arrests and field contacts
- Re-development of weekly CompStat reports to comply with request of Chief William Bratton when he consulted for OPD
- Reconciliation of incident activity and confirmation of accuracy of OPD reporting to CA DOJ and FBI of monthly Uniform Crime Reporting statistics
- Conversion of transcribed citations and hard copy stop data reports for use by Federal monitor to clear Task 34 of NSA
- Ongoing consulting of how Stop Data reports should be recorded in OPD CAD system for optimal reporting as required by Federal Monitor
- Analysis of stop data for use in Federal Monitor reports
- Development of prototype stop data analysis capability that revealed certain geodemographic groups in Oakland may have been disproportionately searched when stopped but such searches resulted in nothing illicit found during search
- Development of prototype officer conduct dashboard that compared officers, patrols and areas using stop data information to determine if there was disproportionate minority contact.

G. Data Security

Forensic Logic constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI Security Management Act of 2003 and CJIS Security Policy[11]. Forensic Logic, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

a. Account Management – OPD personnel who use Forensic Coplink have access accounts that are created, deleted and managed by local Administrators (OPD) with special access permissions to the system. CopLink SEARCH (formerly LEAP) users are managed through a centralized account management process by Forensic Logic support personnel. OPD is working with the Oakland Information Technology Department (ITD) to incorporate the Microsoft Active Directory email authentication protocol, so that the system authenticates when the user has a currently authorized user login identification and password.

b. Microsoft Azure Government Cloud Protocols - Azure Government services handle data that is subject to several CJIS-type government regulations and requirements (e.g. such as FedRAMP (fedramp.gov), NIST 800.171 (DIB)[12], CJIS). One strategy is that Azure Government uses physically isolated datacenters and networks (located in U.S. only). All devices connecting to the Azure infrastructure are authenticated before access is granted. Only trusted devices with registered IP's are permitted to connect. Connections directly to NLETS are only provided via virtual private network (VPN).

c. Encryption - Data in Transit: In accordance with CSP 5.10.1.2.1, all traffic transmitted outside of the secured environment is encrypted with Transport Layer Security (TLS), using RSA[13] certificates and FIPS 140-2 certified cyphers. Data at Rest: All Azure GovCloud storage solutions use Azure Encrypted Managed Disks. No data at rest shall be removed from the secured environment for any reason. Forensic Logic CopLink Data residing on Forensic Logic computers located at the NLETS data center is also encrypted at rest.

d. User Authentication and Authorization - All authorized users must maintain and enter a valid user id/strong password combination to gain access to the system. Passwords must be changed every 90 days and must adhere to Basic Password Standards listed in CSP v5.8 Paragraph 5.6.2.1.1. In addition to user and device authentication mechanisms, the system employs a two-factor advanced

[11] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
[12] https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
[13] RSA is a public key encryption algorithm that cannot be broken in a timely manner by even the largest computer networks: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
https://en.wikipedia.org/wiki/FIPS_140-2

authentication services. These services provide a single use, time-sensitive token, delivered to a mobile device, tablet or computer, which must be entered into the logon process in order to gain access from devices outside of the physically secured location. Upon successful logon, access to specific objects are authorized based on Access Control Lists (ACLs) in accordance with CSP 5.5.2.4

e. Personnel Screening, Training and Administration - In accordance with CSP 5.12.1.1, all Forensic Logic employees are fingerprinted, background checked and required to read and sign the FBI Security Addendum located in Appendix H of the CSP. All employees have also successfully completed Level Four Security Awareness Training in accordance with CSP 5.2.1.4.

H. Costs

.

Commented [BS1]: OPD is currently negotiating the cost of a 2-3 year new contract with Forensic. Prior, OPD paid approximately 185k/yr for services. OPD anticipates a new annual cost at a slightly higher rate.

I. Third Party Dependence

OPD relies on Forensic Logic, Inc. as a private company to provide OPD with access to its data warehouse, search engine, and crime reporting tools. The combination of the prior LEAP Search combined with the CopLink system create a unique product with national scope.

J. Alternatives Considered

No other product or company can realistically provide OPD with both the complex crime report support and search functionality provided by Forensic Logic.

The former Omega Group (now a division of Central Square) provides crimemapping capabilities and is an OPD vendor. Its public facing product is limited to 180 days of visualization; is limited to no more than approximately 500 incidents on a map simultaneously (for reference Oakland had 685 burglaries, 777 auto thefts and 481 aggravated assaults recorded just in May 2020); and not all incidents are visualized as certain incident types are filtered out.

Forensic Logic has built a customized crime report system that reaches back to more than a decade to compare crime types at the agency, area and beat level and is explained above that would require Oakland to expend significant time and resources to replicate even with a new vendor.

In the immediate term, OPD would have less access to its own CAD/RMS data – the current system is very outdated; OPD is in the process of

implementing a new Motorola-based CAD/RMS system[14] but even once that process is complete later in 2020 or 2021, OPD will require continued access to Forensic Logic's much more accessible format for querying OPD CAD/RMS data. The Oakland Police Department has not contracted Motorola to convert the entire history of crime incidents from its existing outdated system to the new CAD/RMS system and therefore, Forensic Logic will retain the only historical searchable information for those incidents not converted into the new CAD/RMS. Similarly, OPD would need to dedicate months of non-available Oakland Information Technology Department (ITD) expertise to develop the algorithms Forensic Logic created to sift and sort OPD CAD/RMS data into usable crime analysis reports upon which the Mayor's Office and the City Council have come to rely.

No other vendor currently provides the local, regional and national law enforcement data needed by OPD to assist in criminal investigations. Authorized OPD personnel could, however, access many types of data contained in Forensic Logic CopLink, without using the Forensic Logic CopLink system. Native OPD systems such as CAD/RMS, Alameda County's CRIMS, OPD Field Based Reporting (or FBR, for recording stop data), and ShotSpotter can be accessed through their direct system portals. However, accessing each system separately takes more time; in the case of current CAD/RMS is complicated and even more time consuming; and does not aggregate the information from the multiple data sources into a common result that provides multi-data set situational awareness. More fundamentally, Forensic Logic CopLink makes each dataset more powerful through connection to data in other systems, where OPD personnel would not otherwise know to connect the data without laborious efforts. For example, if an investigator knows which agency may have useful information, they can contact that agency (e.g., BART Police), and ask the agency to manually query their data system to look for the relevant information. However, in many cases, OPD investigators would not know which agency to call and it would be very difficult to call many agencies to ask for leads in different types of cases.

K. Track Record of Other Entities

Many other police agencies in the Bay Area, in California, and nationally utilize the Forensic Logic CopLink System. In fact, Oakland benefits significantly from the IBM CopLink acquisition by Forensic Logic due to the concentration of California agencies that were customers of CopLink. Data from the California Counties of Orange, Santa Clara, San Mateo, Contra Costa, Stanislaus, Monterey; most of southern Oregon; Las Vegas NV Metro area; all of Arizona are already available to OPD and integrations with the Counties of San Francisco, San Diego, Los Angeles. Santa Barbara, and the

[14] OPD's CAD-RMS contract was finalized in December 2017; a contract for the second phase of work was signed in 2019.

Spokane, WA area are underway.

OPD staff spoke with an investigator with SFPD in the production of this report. The investigator explained that LEAP / CopLink is by far the most useful source of law enforcement data and that this tool makes crime investigations much more effective. In a recent SFPD case related to numerous sexual assaults, SFPD was able to find similar cases in another county that allowed investigators to contact other victims; the other victims provided additional suspect information which was invaluable in the recent arrest of the suspect.

OAKLAND
POLICE DEPARTMENT
455 7th St., Oakland, CA 94607 | OPDCRIMEANALYSIS@OAKLANDNET.COM
CRIME ANALYSIS

Weekly Crime Report—Citywide
20 Apr. — 26 Apr., 2020

Part 1 Crimes *All totals include attempts except homicides.*	Weekly Total	YTD 2018	YTD 2019	YTD 2020	YTD % Change 2019 vs. 2020	3-Year YTD Average	YTD 2020 vs. 3-Year YTD Average
Violent Crime Index (homicide, aggravated assault, rape, robbery)	80	1,636	1,781	1,752	-2%	1,723	2%
Homicide – 187(a)PC	1	17	24	16	-33%	19	-16%
Homicide – All Other *	-	6	2	1	-50%	3	-67%
Aggravated Assault	45	768	848	854	1%	823	4%
Assault with a firearm – 245(a)(2)PC	6	78	88	94	7%	87	8%
Subtotal - Homicides + Firearm Assault	7	101	114	111	-3%	109	2%
Shooting occupied home or vehicle – 246PC	6	75	81	95	17%	84	14%
Shooting unoccupied home or vehicle – 247(b)PC	1	25	37	39	5%	34	16%
Non-firearm aggravated assaults	32	590	642	626	-2%	619	1%
Rape	5	65	70	75	7%	70	7%
Robbery	29	786	839	807	-4%	811	0%
Firearm	12	292	290	244	-16%	275	-11%
Knife	3	50	36	74	106%	53	39%
Strong-arm	8	342	383	380	-1%	368	3%
Other dangerous weapon	1	26	25	21	-16%	24	-13%
Residential robbery – 212.5(a)PC	1	27	31	28	-10%	29	-2%
Carjacking – 215(a) PC	4	49	74	60	-19%	61	-2%
Burglary	65	2,892	4,096	3,865	-6%	3,618	7%
Auto	36	2,158	3,290	3,171	-4%	2,873	10%
Residential	10	497	549	391	-29%	479	-18%
Commercial	13	191	212	210	-1%	204	3%
Other (Includes boats, aircraft, and so on)	2	38	37	47	27%	41	16%
Unknown	4	8	8	46	475%	21	123%
Motor Vehicle Theft	111	2,072	2,053	2,364	15%	2,163	9%
Larceny	49	1,987	2,165	2,029	-6%	2,060	-2%
Arson	1	52	36	46	28%	45	3%
Total	306	8,645	10,133	10,057	-1%	9,612	5%

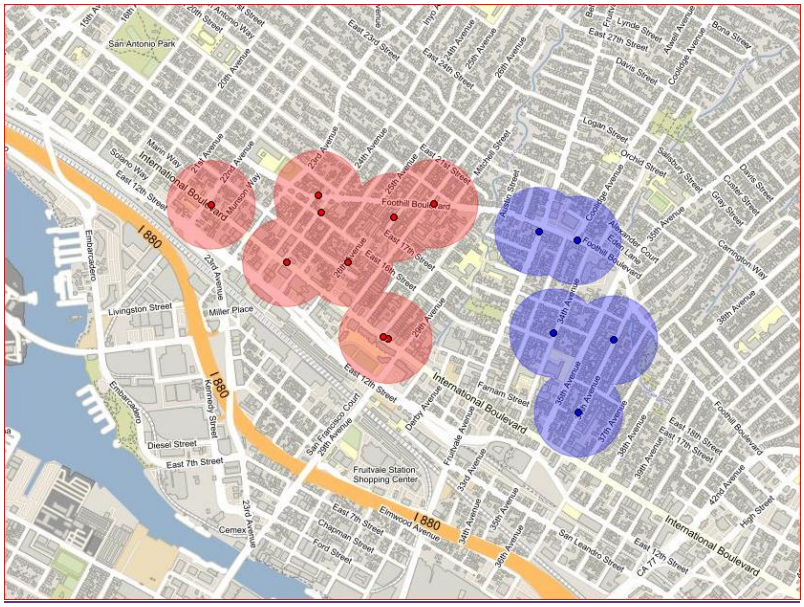
THIS REPORT IS HIERARCHY BASED. CRIME TOTALS REFLECT ONE OFFENSE (THE MOST SEVERE) PER INCIDENT.

These statistics are drawn from the Oakland Police Dept. database. They are unaudited and not used to figure the crime numbers reported to the FBI's Uniform Crime Reporting (UCR) program. This report is run by the date the crimes occurred. Statistics can be affected by late reporting, the geocoding process, or the reclassification or unfounding of crimes. Because crime reporting and data entry can run behind, all crimes may not be recorded.

** Justified, accidental, foetal, or manslaughter by negligence. Traffic collision fatalities are not included in this report.*
PNC = Percentage not calculated — Percentage cannot be calculated.
All data extracted via the LEAP Network.

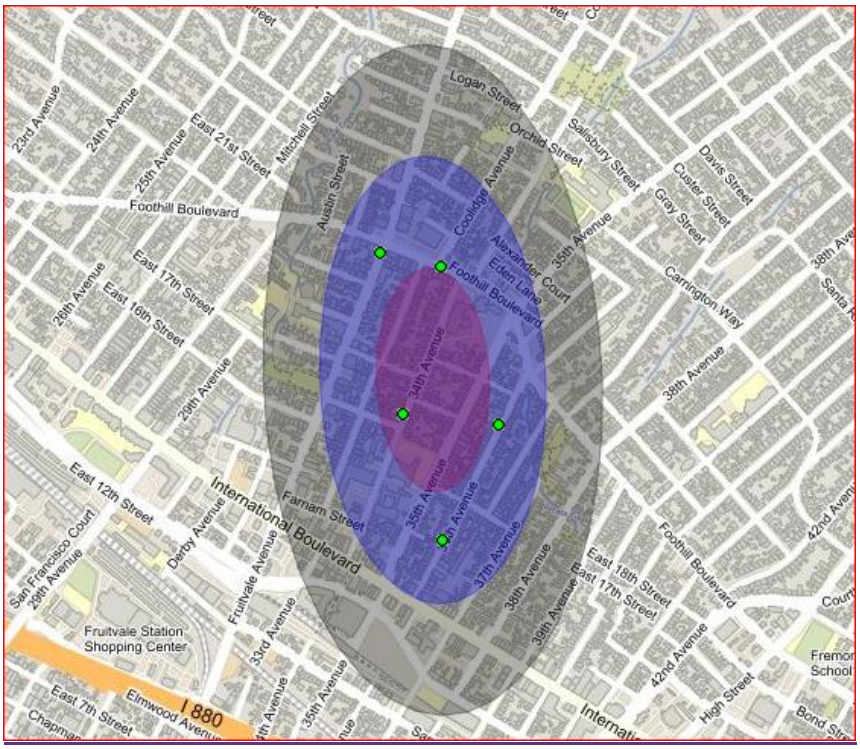
Appendix B

Figure 1: CopLink HotBlocks Feature of Penal Code PC 245(a)(2) shootings in Oakland between January 1, 2020 and May 31, 2020



Appendix C

Figure 2: CopLink Next Crime Location (NCL) Feature of Penal Code PC 245(a)(2) shootings in Oakland between January 1, 2020 and May 31, 2020



This tool similarly allows personnel to see crime density on a map so that personnel can make more informed decisions about where crime is more likely to occur in the future.

DEPARTMENTAL GENERAL ORDER

I-24: FORENSIC LOGIC COPLINK

Effective Date:

Coordinator: Information Technology Unit

FORENSIC LOGIC COPLINK

The purpose of this order is to establish Departmental policy and procedures for the use of the Forensic Logic, LLC. CopLink Data System

VALUE STATEMENT

The purpose of this policy is to establish guidelines for the use of the Forensic Logic, LLC. CopLink law enforcement data search system. The Oakland Police Department (OPD) uses crime databases to provide OPD personnel with timely and useful information to investigate crimes and analyze crime patterns.

A. Purpose: *The specific purpose(s) that the surveillance technology is intended to advance*

Forensic Logic, Inc. ("Forensic Logic") built a data warehouse that integrates and organizes data from databases such as Computer Assisted Dispatch (CAD) and Records Management System (RMS) and other law enforcement information systems from different law enforcement agencies. Forensic Logic provides two core services for OPD: 1) crime analysis reports; and 2) data search.

1. Crime Analysis Report Production – Forensic Logic categorizes and organizes incidents by offense types that allows OPD crime analysts to produce crime analysis reports such as point in time year-to-date and year-to-year comparisons. The categorization takes thousands of penal code types and organizes the data in a comprehensive manner to tabulate data into standard Federal Bureau of Investigation (FBI) Uniform Crime Report Part One and Part Two crimes.
2. Search – OPD data (e.g., CAD/RMS) is searchable with other agency law enforcement data. Personnel can use the system to search crime reports for structured data (e.g., suspect names) and unstructured data (e.g., a vehicle description). The cloud-based search system is accessible via a secure internet web browser requiring user authentication from vehicle mobile data terminal (MDT), web-enabled computers on the OPD computer

network, or via OPD-issued and managed mobile devices.

B. Authorized Use*: The specific uses that are authorized, and the rules and processes required prior to such use*

The authorized uses of Forensic Logic system access are as follows:

- Crime Analysis Report Production – Authorized members may use the customized system to organize OPD crime data into Crime Analysis Reports. Forensic Logic built a system that categorizes thousands of penal codes based on hierarchical crime reporting standards, into a concise, consumable report template.
- CopLink Search – Authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Rules and Processes Prior to use

- Only sworn law enforcement personnel or authorized professional staff employed and working under the supervision of a law enforcement agency (typically crime analysts and dispatchers) may access the Forensic Logic CopLink network.
- OPD personnel authorized to use Forensic Logic CopLink receive required security awareness training prior to using the system. Forensic Logic requires users to have the same training to access the Forensic Logic CopLink network as users are required to be trained to access data in CLETS, the FBI NCIC system or NLETS. Users are selected and authorized by OPD and OPD warrants that all users understand and have been trained in the protection of Criminal Justice Information (CJI) data in compliance with FBI Security Policy. All Forensic Logic CopLink users throughout the Forensic Logic CopLink network have received required training and their respective law enforcement agencies have warranted that their users comply with FBI CJI data access requirements.
- Users shall not use or allow others to use the equipment or database records for any unauthorized purpose; authorized purposes consist only of queries related to authorized investigations, internal audits, or for crime analysts to produce crime analysis reports. The purpose of the Forensic Logic CopLink network is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. Users are required to abide by the Terms of Service of the Forensic Logic CopLink network when they access the system. The Terms of Service that every User agrees to include the following statements:
    1. *I will use the Forensic Logic Coplink Network™ only for the administration of criminal justice or the administration of data required to be stored in a secure sensitive but unclassified data environment.*

2. *I will respect the confidentiality and privacy of individuals whose records I may access.*
3. *I will observe any ethical restrictions that apply to data to which I have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information.*
4. *I agree not to use the resources of the Forensic Logic Coplink Network™ in such a way that the work of other users, the integrity of the system, or any stored data may be jeopardized.*

I am forbidden to access or use any Forensic Logic Coplink Network™ data for my own personal gain, profit, or the personal gain or profit of others, or to satisfy my personal curiosity.

- The following warning is displayed for every user session prior to user sign on:

  WARNING: *You are accessing sensitive information including criminal records and related data governed by the FBI's Criminal Justice Information System (CJIS) Security Policy. Use of this network provides us with your consent to monitor, record, and audit all network activity. Any misuse of this network and its data is subject to administrative and/or criminal charges. CJIS Security Policy does not allow the sharing of access or passwords to the Forensic Logic Coplink Network™. The data content of the Forensic Logic Coplink Network™ will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures or any activity that would directly result in providing sworn testimony in any court by any participating agency. Information available in the Forensic Logic Coplink Network™ is not probable cause, but indicates that data, a report or other information exists in the Records Management System or other law enforcement, judicial or other information system of an identified participating agency or business.*

  In accordance with California Senate Bill 54, applicable federal, state or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644.

- Accessing CopLink data requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in a criminal investigation.

C. ***Data Collection:*** *The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data;*

Forensic Logic has created a file transfer protocol to automatically ingest several data systems into the Forensic Logic CopLink system. These databases include

CAD/RMS and FBR. Additionally, OPD is discussing the possibility of incorporating National Integrated Ballistic Information Network (NIBIN) firearm shell casing data into the system. No ALPR data collected by OPD-owned technology shall be extracted by Forensic Logic's systems. An exhaustive list of data sets ingested by Forensic Logic CopLink from OPD data sources follows.

Data Source Collected	**Collection Status**	**Retention Policy**	**Access Conditions**
Arrest	Active	Perpetual	Only law enforcement; US DHS prohibited
Field Contacts	Active	Perpetual	Only law enforcement; US DHS prohibited
Incident Reports	Active	Perpetual	Only law enforcement; US DHS prohibited
Calls for Service	Active	Perpetual	Only law enforcement; US DHS prohibited
Stop Data	Active	Perpetual	Only law enforcement; US DHS prohibited
Traffic Accident	Active	Perpetual	Only law enforcement; US DHS prohibited
ShotSpotter	Active	Perpetual	Only law enforcement; US DHS prohibited
ATF NIBIN Ballistics	Proposed	Perpetual	Only law enforcement; US DHS prohibited

D. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information*

Authorized users include all sworn personnel, Crime Analysts, Police Evidence Technicians, personnel assigned to OIG, and other personnel as approved by the Chief of Police.

OPD data in the Forensic Logic CopLink system is owned by OPD and not Forensic Logic and is drawn from OPD underlying systems. OPD personnel shall follow all access policies that govern the use of those originating OPD technologies.

OPD's Information Technology (IT) Unit shall be responsible ensuring ongoing compatibility of the Forensic Logic CopLink System with OPD computers and MDT computer systems. OPD's IT Unit will assign personnel to be responsible for ensuring system access and coordinate with Forensic Logic. CopLink Search users are managed through a centralized account management process by Forensic Logic support personnel.

E. *Data Protection:* *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms;*

Forensic Logic constantly processes large streams of criminal justice information (CJI) and thus must comply with the provisions of the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI) and the FBI Security Management Act of 2003 and CJIS Security Policy. Forensic Logic, along with their partner at Microsoft Azure Government and the National Law Enforcement Telecommunications System (NLETS), have developed strong CJIS-compliant data security protocols.

F. *Data Retention**: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;*

Forensic Logic follows the data retention schedules reflective of OPD's data retention schedules. Data that is deleted from OPD CAD/RMS or other systems will be automatically deleted from Forensic Logic CopLink system. OPD can also request that OPD data be expunged from the Forensic Logic CopLink system where appropriate based on changes to incident files.

G. *Public Access**: How collected information can be accessed or used by members of the public, including criminal defendants;*

The Weekly Crime Analysis Reports prepared using Forensic Logic's analysis of OPD crime data are regularly made available to the public on OPD's website. The CopLink system is only provided for OPD personnel and is not available to the public.

Commented [BH1]: This category pertains to data, not a report. This needs to be addressed.

Commented [BS2R1]: The reports are a function of the technology and represent a form of "public access."

H. *Third Party Data Sharing:* *If 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;*

Other than selected individuals with a right to access at ITD, no other non-OPD City entities may access the Forensic Logic system. Many law enforcement agencies

(city police departments and county sheriff offices) utilize Forensic Logic CopLink. ***Attachment A*** to this Use Policy provides a list of ~~-~~agencies[1] that are clients of Forensic Logic and have access to OPD data through CopLink Search.

Many ~~l~~Law enforcement agencies that are clients of Forensic Logic have access to OPD data through CopLink – a complete list is provided in ***Appendix D*** to the CopLink Surveillance Impact Report. ~~in the following CA counties currently either have access and/or contribute or plan to contribute data to the Forensic Logic CopLink network.~~

Commented [BH3]: Huh?

I. ***Training:*** *The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;*

OPD's IT Unit shall ensure the development of training regarding authorized system use and access.

J. ***Auditing and Oversight:*** *The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and*

The OPD IT Unit will manage audit requests in conjunction with Forensic Logic, Inc.

Commented [BH4]: From whom?

Commented [BS5R4]: The intent here it to explain who in OPD is responsible internally rather than detail the actual information of a potential audit, similar to saying that IT unit is responsible for annual report below.

Per FBI CJIS Security Policy, Paragraph 5.4, Forensic Logic logs information about the following events and content and a report can be produced upon request at any time.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
a. access permission on a user account, file, directory or other system resource;
b. create permission on a user account, file, directory or other system resource;
c. write permission on a user account, file, directory or other system resource;

[1] This list represents all agencies who are able to see OPD data. These agencies do not actually necessarily see OPD data; OPD data only comes up in a search result list if something in the record has the same terms as those that a user puts into the search box. The further away from the location of the incident, an OPD record is unlikely to be in the top few results pages unless the exact person is found.

d. delete permission on a user account, file, directory or other system resource;
e. change permission on a user account, file, directory or other system resource.

3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
a. access the audit log file;
b. modify the audit log file;
c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

OPD's IT Unit shall provide the Chief of Police, Privacy Advisory Commission, and City Council with an annual report that covers use of Forensic Logic's CopLink and Crime Reporting modules during the previous year. The report shall include all report components compliant with Ordinance No. 13489 C.M.S.

K. Maintenance: *The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.*

Forensic Logic, Inc. shall be responsible for all system maintenance per the OPD-Forensic Logic, Inc "software as a service" or (SAAS) contract model.

By Order of

Susan E. Manheimer

Chief of Police Date Signed:

Law Enforcement Agencies Enabled to View Oakland CA Police Department Data

Compiled June 14, 2020

Law Enforcement Agencies with Access to OPD Data

Law Enforcement Agency	*State*
Alameda Co DA	CA
Alameda PD	CA
Alameda SO	CA
ATF - Los Angeles Field Division	CA
ATF - San Francisco Field Division	CA
Bart PD	CA
Berkeley PD	CA
CA DOJ Bureau of Gambling	CA
Campbell PD	CA
Capitola PD	CA
Carlsbad Police Department	CA
Carmel PD	CA
Chula Vista Police Department	CA
Clovis PD	CA
Colma PD	CA
Coronado Police Department	CA
CSU San Jose PD	CA
Daly City PD	CA

Law Enforcement Agency	*State*
Del Rey Oaks PD	CA
El Cajon Police Department	CA
Emeryville PD	CA
Escondido Police Department	CA
FBI - San Francisco	CA
Foster City PD	CA
Fremont PD	CA
Fresno PD	CA
Gilroy PD	CA
Greenfield PD	CA
Hayward PD	CA
Hillsborough PD	CA
La Mesa Police Department	CA
Los Altos PD	CA
Los Gatos-Monte Sereno PD	CA
Marina PD	CA
Menlo Park PD	CA
Milpitas PD	CA

Law Enforcement Agency	*State*
Modesto PD	CA
Monterey County DA	CA
Monterey County SO	CA
Monterey PD	CA
Morgan Hill PD	CA
Mountain View PD	CA
National City Police Department	CA
Newark PD	CA
Oakland HA PD	CA
Oakland PD	CA
Oakland USD PD	CA
Oceanside Police Department	CA
Pacifica PD	CA
Palo Alto PD	CA
Piedmont PD	CA
Redwood City PD	CA
Salinas PD	CA
San Bruno PD	CA

Law Enforcement Agencies with Access to OPD Data

Law Enforcement Agency	*State*
San Diego Harbor Police	CA
San Diego Police Department	CA
San Diego Sheriff's Office	CA
San Francisco DA	CA
San Francisco PD	CA
San Joaquin DA	CA
San Jose Evergreen CCD PD	CA
San Jose PD	CA
San Jose State U PD	CA
San Leandro PD	CA
San Mateo PD	CA
San Mateo SO	CA
Santa Clara County DA	CA
Santa Clara County Probation	CA
Santa Clara PD	CA
Santa Clara SO	CA
Santa Cruz County SO	CA
Santa Cruz PD	CA

Law Enforcement Agency	*State*
Seaside PD	CA
South San Francisco PD	CA
Stanislaus SO	CA
Sunnyvale DPS	CA
Tracy PD	CA
Turlock PD CA	CA
Union City PD	CA
USMS - Northern California	CA
Watsonville PD	CA
WSIN	CA
Catoosa County SO	GA
Gardner PD	KS
Johnson SO	KS
Leavenworth PD	KS
Lenexa PD	KS
Overland Park PD	KS
Prairie Village PD	KS
Shawnee PD	KS

Law Enforcement Agency	*State*
Jefferson Parish SO	LA
Kenner PD	LA
Kansas City MO PD	MO
Albany PD	OR
Aumsville PD	OR
Bend PD	OR
Benton County SO	OR
Corvallis PD	OR
Dallas PD	OR
DEA, Portland	OR
DOJ - Oregon	OR
Eugene PD	OR
Gervais PD	OR
Hubbard PD	OR
Independence PD	OR
Keizer PD	OR
Lincoln City PD	OR
Lincoln County SO	OR

Law Enforcement Agencies with Access to OPD Data

Law Enforcement Agency	*State*
Linn County SO	OR
Marion County SO	OR
McMinnville PD	OR
Monmouth PD	OR
Mt. Angel PD	OR
Newberg PD	OR
NORCOM	OR
Oregon DOC	OR
Oregon DOJ	OR
Oregon State Police	OR
Philomath PD	OR
Polk Co Community Corrections	OR
Polk County SO	OR
Salem PD	OR
Silverton PD	OR
Stayton PD	OR
Sweet Home PD	OR
Toledo PD	OR

Law Enforcement Agency	*State*
Turner PD	OR
Woodburn PD	OR
Greenville County SO	SC
ATF - Houston Field Division	TX
El Paso PD	TX
FBI - Houston	TX
Harris SO	TX
Hidalgo Co SO	TX
Houston PD	TX
North Richland Hills PD	TX
AIRWAY HEIGHTS PD	WA
ATF - Seattle Field Division	WA
BONNER COUNTY SO	WA
CHENEY PD	WA
COEUR D'ALENE PD	WA
KOOTENAI COUNTY SD	WA
LIBERTY LAKE PD	WA
SPOKANE COUNTY SO	WA

Law Enforcement Agency	*State*
SPOKANE PD	WA

Exhibit 1

Scope of Work

Forensic Logic will provide the Oakland Police Department (OPD) with a suite of online search, data discovery and analytic tools that facilitate more rapid identification and apprehension of criminal subjects, report and visualize officer disproportionate minority conduct, and provide crime reports for public and in-agency consumption.

The services to be performed by Forensic Logic include (but not limited to) the following:

1. Extraction of data from OPD sources for use in SEARCH engine
2. Mapping of LRMS to UCR and NIBRS standards for weekly reporting
3. Dashboard to analyze DMC activity by OPD officers
4. Weekly CompStat reports (as amended over time)
5. DMC analysis tools

8/23/17

Schedule A

CITY OF OAKLAND
CONSULTING AND PROFESSIONAL SERVICES CONTRACTORS
SCOPE OF WORK/OUTLINE OF SERVICES TO BE PERFORMED

The services to be performed by Consultant shall consist of services requested by the Project Manager or a designated representative, including (but not limited to) the following:

TASK:	COMPLETION:
1. CONTINUE TO PROVIDE EXTRACTION OF DATA FROM OPD SOURCES FOR USE IN LEAP NETWORK SEARCH ENGINE	ONGOING
2. CONTINUE TO PROVIDE MAPPING OF LRMS DATA TO UCR AND NIBRS STANDARDS FOR REPORTING	ONGOING
3. CONTINUE TO PROVIDE THE DASHBOARD TO ANALYZE DMC (STOP DATA) ACTIVITY BY OPD OFFICERS	ONGOING
4. CONTINUE TO PROVIDE THE TOOLS TO PREPARE CRIME REPORTS WEEKLY AND AS-NEEDED – AS AMENDED OVER TIME	ONGOING
5. CONTINUE TO PROVIDE THE DMC (STOP DATA) ANALYSIS TOOL	ONGOING
6. CONTINUE TO PROVIDE MAINTENANCE AND SUPPORT FOR ABOVE	ONGOING

Consultant:

FORENSIC LOGIC LLC
(Please Print)

Robert L Batty, Executive Chairman
(Signature)
(ON BEHALF OF FORENSIC LOGIC LLC)

August 27 2018
(Date)

City Representative:

CAPTAIN ROLAND HOLMGREN
(Please Print)

(Signature)

17 Jul 18
(Date)

ATTACHMENT A
PROFESSIONAL SERVICES
AGREEMENT

PLEASE NOTE:
As you review the following agreement, please consider the following **"Instructions to Respondents Regarding the City's Proposed Contract"**

Exceptions to or waivers of the terms and conditions are not encouraged. However, if respondents believe them necessary, the following procedure must be followed in all such circumstances. Failure to comply with these procedures will disqualify the submission.

Generally

A. All exceptions to or waivers of the terms and conditions taken must be accompanied by a separate request, in writing, setting forth the grounds for the requested exception or waiver.

B The written requests must accompany the proposal and are subject to the rules for timely responses of proposals.

C. The City reserves the right to reject responses based upon a Respondent's exceptions to or requested waiver of the City's terms and conditions.

Respondents' attention is specifically directed to the following:

1. Contract Terms and Conditions

a. Performance Bond

The City of Oakland City Council requires a Performance Bond for all City contracts to establish a source of revenue for completing the project in question should a vendor become insolvent. The City Administrator has the discretion to waive this requirement pursuant to a vendor's request for such waiver, in writing, which establishes to the City Administrator's satisfaction, that the vendor is sufficiently solvent such that the Bond is not needed. The City Administrator's decision as to whether or not to waive the Bond requirement is final.

b. Liquidated Damages for Contractor's Unexcused Untimely Performance

Where time is of the essence in the performance of the contract, Liquidated Damages are required to incent the vendor's timely performance. Liquidated Damages are assessed only for the vendor's unexcused delays in meeting the agreed upon progress objectives for the contract. Exceptions to this provision are rarely granted and must be based upon an alternative that, in the City's sole

discretion, incents and assures the timely performance of the contract. Exceptions not granted will disqualify the proposal from further consideration.

2. Contract Compliance Provisions

The City's Contract Compliance provisions have been established by the Contract Compliance Department. All exceptions taken to those provisions will require a written request to grant the exception and should be submitted to:

Deborah Lusk-Barnes
Director, Contracts & Compliance, Office of the City Administrator
250 Frank Ogawa Plaza, Suite 3341
Oakland, Ca. 94612
(510) 238-6270 dbarnes@oaklandnet.com

The request for each exception taken must accompany the Respondent's submittal and must clearly set forth why the exception should be granted. Contract Compliance will review each requested exception and has the sole discretion to grant it or not. Exceptions not granted will disqualify the proposal from further consideration.

3. City Schedules

The City's Schedules have been established pursuant to City Council action, are mandatory and must be completed without modification and submitted with your proposal. Failure to do so will disqualify the proposal from further consideration.

ATTACHMENT A (Continued)
PROFESSIONAL SERVICES
AGREEMENT
BETWEEN THE CITY OF OAKLAND
AND FORENSIC LOGIC, LLC

TABLE OF CONTENTS

32. Counterparts
33. Remedies Cumulative
34. Severability/Partial Invalidity
35. Access
36. Entire Agreement of the Parties
37. Modification
38. Notices
39. Right to Offset
40. No Third Party Beneficiary
41. Survival
42. Time is of the Essence
43. Authority

EXHIBITS

Exhibit 1 **Statement of Work / Scope of Work**
Exhibit 2 **Bill of Materials**
Exhibit 3 **Maintenance Agreement**
Exhibit 4 **Contractor's RFP Proposal and Project Proposal Presentation**
Exhibit 5 **Contract Compliance Provisions**

1. Business Tax Certificate
2. Inspection of Books and Records/Right to Audit
3. Non-Discrimination/Equal Employment Practices
4. Americans with Disabilities (ADA Requirements)
5. Local, Small Business Enterprise Program (LSBE)
6. Other Applicable Ordinances
7. City of Oakland Campaign Contribution Limits
8. Insurance
9. Political Prohibition
10. Religious Prohibition

Exhibit 6—City Schedules

1. Schedule B – Billing Rate
2. Schedule B-2 -Arizona Resolution
3. Schedule C-1_P_U_V - Combined Form
   a. Schedule C-1 - Compliance With The Americans With Disabilities Act
   b. Schedule P - Nuclear Weapons Proliferation Ordinance
   c. Schedule U - Compliance Commitment Agreement
   d. Schedule V - Affidavit Of Non-Disciplinary Or Investigatory Action
4. Schedule D - Ownership, Ethnicity and Gender Questionnaire
5. Schedule E - Project Consultant Team Form
6 Schedule K – Pending Dispute Disclosure Form
7. Schedule M -
   a. Part A - Independent Employer Questionnaire – Vendor completed

b. Part B - Independent Employer Questionnaire -- Requesting Department completed

8. Schedule N - Declaration Of Compliance With Living Wage Ordinance (Professional Services and Design Build Projects only)
9. Schedule N-1 - Equal Benefits Declaration Of Nondiscrimination
10. Schedule O - Disclosure of Campaign Contributions Form
11. Schedule Q - Professional & Specialized Services Insurance Requirements
12. Schedule W – Broder Wall Prohibition Form

AGREEMENT TO PROVIDE
PROFESSIONAL SERVICES AND RELATED PRODUCTS
BETWEEN THE CITY OF OAKLAND
AND FORENSIC LOGIC

This Agreement to provide Professional Services and Related Products as applicable and as set for with specificity herein ["Agreement"] is entered into as of the date when fully executed below between FORENSIC LOGIC LLC ("Contractor") and the City of Oakland ("City"), a municipal corporation, One Frank H. Ogawa Plaza, Oakland, California 94612, who agree as follows:

RECITALS

This Agreement is made with reference to the following facts and objectives:

A. **WHEREAS,** the City Council has authorized the City Administrator to enter into contracts for professional or specialized services if the mandates of Oakland City Charter Section 902(e) have been met; and

B. **WHEREAS,** Contractor is the developer or distributor of software products, hardware and provides related professional services ["Services"]; and

C. **WHEREAS,** City is part of and provides information technology services to the various City departments, offices, and programs; and

D. **WHEREAS,** City wishes to acquire Contractor's Services as specifically set forth in this Agreement, including the Statement of Work ["SOW"] attached hereto and

E. **WHEREAS,** the following Exhibits and Schedules are attached to and incorporated by reference into this Agreement:

Exhibit 1	**Statement of Work**
Exhibit 2	**Bill of Materials**
Exhibit 3	**Maintenance Agreement**
Exhibit 4	**Performance Bond**
Exhibit 5	**Contractor's RFP Proposal and Project Proposal Presentation**
Exhibit 6	**Contract Compliance Provisions**
Exhibit 7	**City Schedules**

NOW THEREFORE, THE PARTIES TO THIS Agreement COVENANT AND AGREE AS FOLLOWS:

1. **Definition**

a. **"Acceptance"** as used herein shall mean the acceptance of Services by City in writing in accordance as provided in Section [INSERT] and Section [INSERT] of Exhibit 1, the Statement of Work ["SOW"] confirming that the Services and Deliverables comply in all material respects with the Specifications.

b. **"Acceptance Certificate"** as used herein shall mean the document substantially in the form of Attachment 1 to the SOW which City shall issue to Contractor when Contractor satisfactorily completes the Testing and Acceptance provisions for Contractor's Deliverables or Services; an Acceptance Certificate must accompany each invoice Contractor submits to City;

c. **"Payment"** as used herein shall mean City's payment to Contractor for Deliverables or Services pursuant to an invoice accompanied by an Acceptance Certificate indicating City has accepted the invoiced Deliverables or Services as provided in Section INSERT] and Exhibit 1; "

e. **OTHERS AS THE PARTIES DEEM APPROPRIATE, E.G. DELIVERABLES, SERVICES, SPECIFICATIONS, REQUIREMENTS, TECHNICAL TERMS;**

2. **Priority of Documents**

In the event of conflicting provisions as between the following documents, except as otherwise expressly stated, the provisions shall govern in the following order: the Amendments to this Agreement, Change Notices (as defined in Section 12 of this Agreement) in reverse chronological order of adoption, this Agreement and its Exhibits. The Exhibits shall govern in numerical order as set out in this Agreement.

3. **Conditions Precedent**

a Contractor must provide City with the following before the Agreement will become effective:

(1). A copy of Contractor's City of Oakland Business Tax License which must be kept current for the duration of the Agreement and shall be attached to this Agreement as part of Exhibit 5;

(2). A completed set of the City of Oakland Schedules which shall be attached to this Agreement as Exhibit 5;

(3) A copy of Contractor's Performance Bond which shall be attached to this Agreement as Exhibit 4 and incorporated herein by this reference.

b. Contractor and City must complete and agree upon and execute a Statement of Work before the Agreement will become effective and which shall be attached to this Agreement and incorporated herein by this reference.

4. Statement of Work

Contactor agrees to perform the services ("**Services**") and provide the deliverables ("**Deliverables**") specified in **EXHIBIT 1 (Schedule A)** the Statement of Work, which is attached to this Agreement and incorporated herein by this reference.

5. Initial Term

The Initial Term of this Agreement is July 01, 2018 through June 30, 2020, and shall start when it is executed in full by all Parties and end on June 30, 2020 upon the satisfactory completion of all tasks set forth in the SOW, and the provision of all Services called for hereunder, unless extended by the written Agreement of the Parties or sooner terminated as provided herein.

6. City Requirements for Project Deliverables

a. As is set forth with specificity in the Statement of Work [Exhibit 1/Schedule A], this Project will require Contractor to provide the Services necessary deliver the Forensic Logic suite of information search and analysis services relative to the project and the Work.

b. This Project is part of the Crime Analysis demands to continue to provide, develop and deploy a comprehensive technology known as LEAP Search and Analysis that integrates key City of Oakland data collection and retrieval which is essential to enhanced consolidated access to internal and external law enforcement data sources,

c. Contractor will be responsible for the entire Scope as set forth in Exhibit 1/Schedule A, the SOW, including, but not limited to being solely responsible for coordinating the activities of all team members, and ensuring that the Scope is fulfilled to the City's satisfaction in accordance with this Agreement.

d. Contractor must provide a turnkey solution for the Project at a firm, fixed price which shall, in no event, exceed $158,000.00 for the First Year (July 01, 2018 - June 30, 2019), and $168,000.00 for the second Year (July 01, 2019 – June 30, 2020), for a total amount of $326,000.00 per Resolution 87193 C.M.S.

7. Contractor Warranty and Indemnification of Services

a. In recognition of City's reliance on its Services and the Special Circumstances of this Project, Contractor warrants that its Services will be suitable for the purpose intended and fully meet City's Requirements. Subject to applicable City of Oakland Section [Limitation on Liability], Contractor agrees to fully indemnify City for all liabilities, claims, losses, damages and expenses, including without limitation, reasonable attorney's

fees, arising from any failure by Contractor in the performance of the Services as required hereunder.

b. Contractor acknowledges that City is a provider of public and municipal services to the public and residents of the City of Oakland and that City's reliance on and use of Contractor's Deliverables will be vital to: (a) the business operations of the City; (b) the orderly and efficient provision of public and municipal services by the City; and (c) the health and safety of City's residents; and therefore, that any unauthorized interruption of City's business and operations could result in substantial liability to City. In recognition of City's status as a provider of such public and municipal services, Contractor warrants and represents that Contractor shall not at any time during the term of this Agreement and thereafter render the Software unusable or inoperable, take possession of the Deliverables provided to City by Contractor or Contractor's subcontractors or in any way deliberately take actions limiting Contractor's liability under this Agreement. If Contractor takes any such actions, Contractor shall be liable for and indemnify City for all liabilities, claims, losses, damages and expenses, including without limitation, reasonable attorney's fees, arising from Contractor's actions the Services and Deliverables (a) will be free from defects in design, workmanship and materials, delivered to City hereunder; (b) will conform in all material respects to the Specifications

c. Contractor represents that it will use all reasonable efforts, including appropriate testing, to ensure that the Software does not contain viruses, contaminants, or other harmful code that may harm the Software, City systems or other City software.

d. Contractor represents that it owns or has the unencumbered right to license and/or assign to City, as provided in this Agreement, the Deliverables and all results of Services delivered to City hereunder, including all required Intellectual Property Rights therein

e. Contractor represents that it has the requisite experience, certifications, skills and qualifications necessary to perform the Services in: (i) a timely, competent, and professional manner, and (ii) accordance with applicable governmental requirements, statutes, regulations, rules and ordinances including, without limitation, applicable data privacy laws and regulations ("Law");

f. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES MADE IN THIS AGREEMENT, THE CONTRACTOR MAKES NO REPRESENTATION, ACKNOWLEDGEMENT, CONDITION OR WARRANTY OF ANY KIND WHATSOEVER UNDER THIS AGREEMENT OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY STATUTORY, EXPRESS, IMPLIED OR OTHER WARRANTIES OR ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE REGARDING ANY SERVICES, DELIVERABLE OR ANY OTHER PRODUCT DELIVERED TO THE CITY UNDER THIS AGREEMENT.

8. **Payments.**

a. Upon performance of the Services (as defined in Section 4 and 6 of this Agreement and in the Statement of Work) and the completion of each Deliverable (as defined in Section 8 of this Agreement and in the Statement of Work) which City has previously Authorized (as defined in Section 3 and 8 (b) and (c) of this Agreement), and City's Acceptance (as defined in Section 8(c) of this Agreement) of that Deliverable, Contractor will invoice City for the Services and Deliverable. The invoice must be accompanied by an Acceptance Certificate (as defined in Section 9.3(b) of this Agreement) for the Services or Deliverable being invoiced. City will pay Contractor's invoice within thirty (30) days of City's receipt of Contractor's invoice. All such payments from the City shall be in immediately available funds and in U.S. dollars. Any amounts invoiced for Deliverables for which City has provided its Acceptance which the City has not paid within 30 days of City's receipt of Contractor's invoice shall accrue interest at the rate of six percent (6%) per annum until paid in full.

b. For the purposes of this Agreement:

(i) "Authorized" shall mean that the City has reviewed the proposed project plan ["Project Plan"] with Contractor during the bi-weekly meetings between the Parties as set out in the Statement of Work attached to this Agreement as Exhibit 1 ("SOW") and has provided written approval to Contractor to continue providing the Services and Deliverables contemplated under the Project Plan.

(ii) "Acceptance" or "Accepted" shall mean that the City has reviewed the Authorized Services or Deliverables upon Contractor's completion of same and accepted them, in writing, in accordance with Section 9 of this Agreement and as provided in the SOW.

c. Contractor acknowledges and agrees that City shall have no obligation whatsoever to pay Contractor for any Services or Deliverables performed which have not been Authorized by the City as contemplated herein. Contractor further acknowledges and agrees that City shall have no obligation whatsoever to pay Contractor for any Services or Deliverables it has not Accepted as provided herein (Acceptance, Section 9).

9. Acceptance

9.1 Unless otherwise agreed in writing, the Parties agree that:

(a) When Contractor completes each Authorized Deliverable ("Deliverable"), the City shall have five (5) Business Days, or such longer period of time as the Parties may agree upon or as is set out in the SOW (the "Acceptance Period"), from the City's receipt of the Deliverable to review and either provide its Acceptance of the Deliverable and an Acceptance Certificate or written notice of its rejection setting out

in detail the reasons why such Deliverable failed to be Accepted in accordance with Section 9.2 of this Agreement;

(b) For each Deliverable, when corrective action is required by the City's written notice of deficiencies, Contractor shall have five (5) Business Days, or such longer period of time as the Parties may agree upon, to correct the deficiencies City has identified as provided herein ["Corrective Action Period"];

(c) For each Deliverable, Contractor shall be given at least two opportunities to correct the deficiencies identified by the City, unless the Parties otherwise mutually agree;

(d) Contractor shall correct any deficient Deliverables for which the City has delivered written notice to Contractor as set out in subsection 9.1(b) above such that the Deliverable complies with the requirements set out under this Agreement,

(e) If Contractor fails to remedy a deficient Deliverable after both opportunities to remedy as set out in subsection 9.1(d) above, then such failures shall constitute a material default of this Agreement; and

(f) Changes to Deliverables for which the City has provided Acceptance will be handled through the Change Notice process set out at Section 12 of this Agreement and Contractor will start no work on any change until the Parties have approved and executed any applicable Change Notice.

9.2 Upon delivery by Contractor of any Deliverable and within the Acceptance Period, the City shall review such Deliverable to determine if such Deliverable meets the applicable Acceptance Criteria as set out in the SOW, and

(a) if such Deliverable meets the applicable Acceptance Criteria or is otherwise, used or acted upon by the City, the Deliverable will be deemed Accepted on such date unless City has given notice to Contractor that it needs to use or act upon the Deliverable in order to determine whether or not it is acceptable,

(b) if such Deliverable does not meet the applicable Acceptance Criteria, the City will provide written notice by no later than the end of the Acceptance Period to Contractor setting out reasonable particulars of any deficiency and Contractor will, within the Corrective Action Period, re-work the Deliverable to meet the applicable Acceptance Criteria, or

(c) if the City fails to provide written notice rejecting the Deliverable, or fails to respond to Contractor in writing by the end of the Acceptance Period, then the City will be deemed to have Accepted such Deliverable.

(d) Once the City Accepts a Deliverable under the terms of this Section 9, including its subparts, City will issue Contractor an Acceptance Certificate which must accompany Contractor's invoice to City for that Deliverable.

9.3 For the purposes of this Agreement:

a. "Acceptance Criteria" means reasonable and objective criteria jointly established and agreed to in writing by the City and Contractor describing the criteria for the completion and acceptability of Deliverables all as more particularly set out in the SOW;

b. "Acceptance Certificate" means a certificate authorized and signed by the City indicating that the City has Accepted the specific Deliverable or Service to which the Acceptance Certificate relates,

10. Proprietary or Confidential Information of the City

10.1 Confidentiality Obligations. Confidential Information shall mean all proprietary or confidential information disclosed or made available by the other Party pursuant to this Agreement that is identified as confidential or proprietary at the time of disclosure or is of a nature that should reasonably be considered to be confidential, and includes but is not limited to the terms and conditions of this Agreement, and all business, technical and other information (including without limitation, all product, services, financial, marketing, engineering, research and development information, product specifications, technical data, data sheets, software, inventions, processes, training manuals, know-how and any other information or material), disclosed from time to time by the disclosing Party to the receiving Party, directly or indirectly in any manner whatsoever (including without limitation, in writing, orally, electronically, or by inspection); provided, however, that Confidential Information shall not include the Content that is to be published on the website(s) of either Party.

10.2 Each Party agrees to keep confidential and not disclose to any third party and to use only for purposes of performing or as otherwise permitted under this Agreement, any Confidential Information. The receiving Party shall protect the Confidential Information using measures similar to those it takes to protect its own confidential and proprietary information of a similar nature but not less than reasonable measures. Each Party agrees not to disclose the Confidential Information to any of its Representatives except those who are required to have the Confidential Information in connection with this Agreement and then only if such Representative is either subject to a written confidentiality agreement or otherwise subject to fiduciary obligations of confidentiality that cover the confidential treatment of the Confidential Information.

10.3 Exceptions.

a. The obligations of this Section 10.3 shall not apply if receiving Party can prove by appropriate documentation, where appropriate, that such Confidential Information (i) was known to the receiving Party as shown by the receiving Party's files at the time of disclosure thereof, (ii) was already in the public domain at the time of the disclosure thereof, (iii) entered the public domain through no action of the receiving Party

subsequent to the time of the disclosure thereof, (iv) is or was independently developed by the Contractor without access to or use of the Confidential Information; (v) was provided to the Contractor by a third party who, to the best of the Contractor's knowledge, was not bound by any confidentiality obligation related to such Confidential Information; or (vi) is required by law or government order to be disclosed by the receiving Party, provided that the receiving Party shall (i) notify the disclosing Party in writing of such required disclosure as soon as reasonably possible prior to such disclosure, (ii) use its commercially reasonable efforts at its expense to cause such disclosed Confidential Information to be treated by such governmental authority as trade secrets and as confidential.

10.4 Contractor acknowledges that City is subject to public disclosure laws and that City will comply with requests for information ("RFI"), as it is required to do under the federal Freedom of Information Act, California Public Records Act, City of Oakland Sunshine Act or judicial or administrative court order. Contractor acknowledges that an RFI may pertain to any and all documentation associated with City's use of Contractor' Services. Contractor further acknowledges that it is obligated to assist and cooperate with City by producing all documentation that is responsive to the RFI so that City may comply with its statutory obligations. City agrees to give Contractor as timely written notice as possible of the RFI such that Contractor may oppose the RFI or exercise such other rights at law as Contractor believes it has. However, Contractor must produce all RFI responsive documents to City and City will comply with the RFI unless, within the time frame established by the statute, judicial or court order under which the RFI is made, Contractor procures a Temporary Restraining Order or similar injunctive relief from a court or other tribunal of competent jurisdiction ordering City not to comply with the RFI pending final determination of Contractor protest of the RFI. Contractor further agrees to accept City's tender of defense and to defend City and pay all City costs of defense in any litigation brought against City with respect to City not complying with an RFI that Contractor protests and will hold City harmless against any claims, attorneys' fees, damages, fines, judgments, or administrative penalties, which may arise from any such ac*tions*.

11. Ownership of Results

Any interest of Contractor or its Subcontractors, in specifications, studies, reports, memoranda, computation documents in drawings, plans, sheets prepared by Contractor or its Subcontractors under this Agreement shall be assigned and transmitted to the City. However, Contractor may retain and use copies for reference and as documentation of its experience and capabilities. To be clear, Contractor delivers an information service to the City over the Internet and all Intellectual Property associated with the curation, organization, or deployment of information as part of Contractor's service will remain the sole intellectual property of Contractor. In addition, copyrights on Contractor web based applications and services user interfaces and application software will remain the intellectual property of Contractor.

12. Change Notices

(a) Upon fifteen (15) days' written notice to Contractor, City shall have the right to request changes in the provision of any future Deliverables under this Agreement by delivering to Contractor a change notice ("Change Notice"), provided that any and all such changes shall be subject to Contractor's written consent. Each Change Notice may specify changes to the Software Contractor is to provide hereunder and the manner in which Contractor is to provide the Software. If any Change Notice causes an increase or decrease in the price or the time required for performance under this Agreement, an equitable adjustment jointly agreed upon by City and Contractor shall be made and the Agreement shall be modified in writing accordingly.

(b) Change Notices issued under this Agreement must be accepted or rejected in writing by Contractor within ten (10) days of Contractor's receipt of its issuance. Notwithstanding as may be otherwise provided here in, if for any reason Contractor should fail to timely accept or reject a Change Notice in writing, such Change Notice shall be deemed accepted.

13. Liquidated Damages for Contractor's Unexcused, Untimely Performance

Contractor's failure to complete the Work within the time allowed will result in the City sustaining damages and the assessment by City of Liquidated Damages.

(a) Excusable Delays (Force Majeure)

If Contractor or City experiences an Excusable Delay Event, Contractor or City shall, within ten (10) days after first becoming aware of each such event, give written notice of the delay to the other party and describe any impact the "Excusable Delay" may have upon the Schedule. If the foregoing Notice(s) are issued, or in the absence thereof from the City, then Contractor shall be entitled to a day for day extension to the Schedule corresponding to the number of days of delay directly caused by the Excusable Delay Event.

(b) Schedule of Liquidated Damages.

City and Contractor recognize that time is of the essence in the performance of this Agreement and that City will suffer financial loss in the form of contract administration expenses (including project management and consultancy expenses), delay and loss of public use, if Contractor does not complete its Services and the Deliverables associated therewith within the respective times specified in this Agreement and in the SOW, plus any extensions that are allowed in accordance with this Agreement. Contractor and City agree that because of the nature of the Services as provided by this Agreement, it would be impractical or extremely difficult to fix the amount of actual damages incurred by City because of the delay in completion or timely delivery of the Services. Accordingly, City and Contractor agree that Contractor shall pay City the following liquidated damages measures:

(i) Deliverables: $500.00 for each calendar day that expires after the time specified in the Scope of Work for Contractor to provide and for City to accept the Deliverables specified in the SOW.

(ii) Milestones: $1,000.00 for each calendar day that expires after the time specified in this Agreement for Contractor to complete the Milestone set forth in this Agreement and to complete all of the Services, excluding all "inexcusable delay" events

14. Limitation on Liability

(a) Either party's liability to the other party for any and all liabilities, claims or damages arising out of or relating to this Agreement, howsoever caused and regardless of the legal theory asserted, including breach of contract or warranty, tort, strict liability, statutory liability or otherwise, shall not, in the aggregate, exceed $4Million or the total value of this Agreement, whichever is greater.

(b) In no event shall either party be liable to the other for any punitive, exemplary, special, indirect, incidental or consequential damages (including, but not limited to, lost profits, lost business opportunities, loss of use or equipment down time, and loss of or corruption to data) arising out of or relating to this Agreement, regardless of the legal theory under which such damages are sought, and even if the parties have been advised of the possibility of such damages or loss.

(c) This limitation of liability shall not apply to all actions, demands, or claims by any third party for death, bodily injury, damage to tangible property in connection with or arising under this Agreement, nor to any intentional misconduct, recklessness, or gross negligence or to Contractor's Confidentiality (Section 10) and indemnification (Section 16) obligations as set forth in this Agreement.

15. Performance Bond

Prior to this Agreement being effective and binding on the City, Contractor shall file with City Clerk and with the City representative to whom Notices should be sent as is specified below in Section [INSERT] ("Notices") a Corporate surety bond, in the form of a Performance Bond, in the penal sum of 100% of the total contract amount of this Agreement to guarantee both faithful performance of Contractor's Services and a source of revenue for the City to complete the Services under this Agreement should Contractor default or become insolvent. City's representative shall attach a copy of the Bond to this Agreement as Exhibit 4. Contractor must keep the Performance Bond current for the duration of this Project.

16. Indemnification

(a) General Indemnification. Notwithstanding any other provision of this Agreement, Contractor shall indemnify and hold harmless (and at City's

request, defend) City, and each of their respective Councilmembers, officers, partners, agents, and employees (each of which persons and organizations are referred to collectively herein as "Indemnitees" or individually as "Indemnitee") from and against any and all liabilities (of every kind, nature and description), claims, lawsuits, losses, damages, demands, debts, liens, costs, judgments, obligations, administrative or regulatory fines or penalties, damages, (incidental or consequential) costs, actions or causes of action, and expenses, including reasonable attorneys' fees, (collectively referred to herein as "Actions") caused by or arising out of any:

(i) Breach of Contractor's obligations, representations or warranties under this Agreement;

(ii) Act or failure to act in the course of performance by Contractor under this Agreement;

(iii) Negligent or willful acts or omissions in the course of performance by Contractor under this Agreement;

(iv) Claim for personal injury (including death) or property damage to the extent based on the strict liability or caused by any negligent act, error or omission of Contractor;

(v) Unauthorized use or disclosure by Contractor of Confidential Information as provided in Section 10 above.

(b) Proprietary Rights Indemnity. Contractor shall indemnify, defend, save and hold harmless Indemnitees from any and all Actions arising out of claims that the Software, infringes upon or violates the Intellectual Property Rights of others. If the Software will become the subject of an Action or claim of infringement or violation of the Intellectual Property Rights of a third party, City, at its option shall require Contractor, at Contractor's sole expense to: (1) procure for City the right to continue using the Software; or (2) replace or modify the Software so that no infringement or other violation of Intellectual Property Rights occurs, if City determines that: (A) such replaced or modified Software will operate in all material respects in conformity with the then-current specifications for the Software; and (B) City's use of the Software is not impaired thereby. Contractor's obligations under this Agreement will continue uninterrupted with respect to the replaced or modified Software as if it were the original Software.

(c) For the purposes of the indemnification obligations set forth herein, the term "Contractor" includes, without limitation, Contractor, its officers, directors, employees, representatives, agents, servants, sub consultants, and subcontractors.

(d) Contractor acknowledges and agrees that it has an immediate and independent obligation to indemnify and defend Indemnitees from any Action which potentially falls within this indemnification provision, which obligation shall arise at the time an Action is tendered to Contractor by City and continues at all times thereafter, without regard to any alleged or actual contributory negligence of any Indemnitee. Notwithstanding anything to the contrary contained herein, Contractor's liability under this Agreement shall not apply to any Action arising from the sole negligence, active negligence or willful misconduct of an Indemnitee.

(e) City shall give Contractor prompt written notice of any Action and shall fully cooperate with Contractor in the defense and all related settlement negotiations to the extent that cooperation does not conflict with City's interests. Notwithstanding the foregoing, City shall have the right, if Contractor fails or refuses to defend City with Counsel acceptable to City, to engage its own counsel for the purposes of participating in the defense. In addition, City shall have the right to withhold payments due Contractor in the amount of reasonable defense costs actually incurred. In no event shall Contractor agree to the settlement of any claim described herein without the prior written consent of City.

(f) All of Contractor's indemnification obligations hereunder are intended to apply to the fullest extent permitted by law (including, without limitation, California Civil Code Section 2782) and shall survive the expiration or sooner termination of this Agreement.

(g) Contractor's indemnification obligations hereunder shall not be limited by the City's insurance requirements contained in Schedule B hereof, or by any other provision of this Agreement.

17. Termination

(a) Termination for Breach. If Contractor breaches any material obligation under this Agreement and fails to cure the breach within 30 days of receipt of written notice from City of said breach, City may terminate the Agreement and, at its option: (i) subject to the Limitation on Liability (Section 14), recover all direct damages it incurs as a result of Contractor's breach; (ii) require that Contractor repay City all monies City has paid Contractor under this Agreement or (iii) retain the portion of Contractor's Deliverables that the City has accepted and paid Contractor for and complete performance of the Agreement with another vendor. In the event City elects to complete performance of the Agreement with another vendor, Contractor shall remain liable for any increase in costs to City of completing the Agreement in excess of the price City would have paid Contractor for completing the Agreement.

(b) Contractor may terminate this Agreement if City breaches a material provision of the Agreement and does not cure the breach within 30 days of written notice from Contractor of said breach. In such event, Contractor will be entitled to payment for Deliverables which City has accepted in accordance with the Testing and Acceptance provisions of this Agreement.

(c) Bankruptcy. Either party may immediately terminate this Agreement if (i) the other party files a petition for bankruptcy or has filed against it an involuntary petition for bankruptcy which is not dismissed within 60 days of its filing, (ii) a court has appointed a receiver, trustee, liquidator or custodian of it or of all or a substantial part of the other party's property, (iii) the other party becomes unable, or admits in writing its inability, to pay its debts generally as they mature, or (iv) the other party makes a general assignment for the benefit of its or any of its creditors.

(d) Termination for Convenience by City. City may terminate this Agreement for any reason at any time upon not less than sixty (60) days' prior written notice to Contractor. After the date of such termination notice, Contractor shall not perform any further services or incur any further costs claimed to be reimbursable under this Agreement, any Purchase Order, Change Order, or Change Notice without the express prior written approval of City. As of the date of termination, City shall pay to Contractor all undisputed amounts then due and payable under this Agreement.

(e) Transition Services after termination. In connection with the expiration or other termination of this Agreement or the expiration of this Agreement, Contractor may provide transition services as requested by City. Such transition services shall be subject to the pricing provided in this Agreement or any amendment thereto.

18. Dispute Resolution

a. If dispute or disagreement among the Parties arises with respect to either Party's performance of its obligations hereunder, or any provision of or interpretation of the Agreement, the Parties agree in good faith to attempt to resolve such dispute or disagreement (a "Dispute") prior to submitting the Dispute to mediation, arbitration or litigation in accordance with this Section 18. Such resolution efforts shall involve the City Administrator of the City of Oakland and an executive officer of Contractor, together with such other persons as may be designated by either Party.

b Any Party may commence said resolution efforts by giving notice, in writing, to any other Party. Such notice shall include at least a description of the Dispute and any remedial action that the Party commencing the resolution procedure asserts would resolve the Dispute. Upon receiving such notice, the Party against whom the Dispute is brought shall respond in writing within five (5) Business Days. The Parties shall then meet and confer in a good faith attempt to resolve the Dispute.

c If the Dispute has not been resolved within five (5) Business Days after the Subsection 18.b. notice is given, and unless the Party initiating the Dispute does not wish to pursue its rights relating to such Dispute or desires to continue the Pre-Mediation Dispute Resolution, then such Dispute will be automatically submitted to mediation. The mediation will be conducted in Alameda County by a single mediator selected by the Parties to the Dispute by mutual agreement or by the use of the Commercial Arbitration Rules of the American Arbitration Association for selecting an Arbitrator ["AAA RULES"] The Parties to the Dispute shall evenly share the fees and costs of the mediator. The mediator shall have twenty (20) Business Days from the submission to mediation to attempt to resolve such Dispute. If the Dispute is not resolved within that time period, the parties will be entitled to pursue such matter by demanding arbitration under the AAA RULES or instituting litigation.

19. Commencement, Completion and Close-out

It shall be the responsibility of the Contractor to coordinate and schedule the work to be performed so that commencement and completion take place in accordance with the provisions of this Agreement.

Any time extension granted to Contractor to enable Contractor to complete the work must be in writing and shall not constitute a waiver of rights the City may have under this Agreement.

Should the Contractor not complete the work by the scheduled date or by an extended date, the City shall be released from all of its obligations under this Agreement.

Within thirty (30) days of completion of the performance under this Agreement, Contractor shall make a determination of any and all final costs due under this Agreement and shall submit a requisition for such final and complete payment (including without limitations any and all claims relating to or arising from this Agreement) to the City. Failure of the Contractor to timely submit a complete and accurate requisition for final payment shall relieve the City of any further obligations under this Agreement, including without limitation any obligation for payment of work performed or payment of claims by Contractor.

20. Bankruptcy.

All rights and licenses granted to City pursuant to this Agreement are, and shall be deemed to be, for purposes of Section 265(n) of the U.S. Bankruptcy Code, licenses of rights to "intellectual property" as defined under Section 101 of the U.S. Bankruptcy Code. In a bankruptcy or insolvency proceeding involving Contractor, the parties agree that City, as licensee of such rights, shall retain and fully exercise all of its rights and elections under the U.S. Bankruptcy Code, and the provisions thereof shall apply notwithstanding conflict of law principles. The parties further agree that, in the event of the commencement of a bankruptcy or insolvency proceeding by or against Contractor under the U.S. Bankruptcy

Code, City shall be entitled to a complete duplicate of any such intellectual property, including the source code for Contractor's Licensed Software which Contractor has placed in escrow as required under this Agreement and all embodiments of such intellectual property, to which City would otherwise be entitled under this Agreement, and the same, if not already in City's possession, shall be promptly delivered to City (a) upon any such commencement of a bankruptcy proceeding upon written request therefore by City, unless Contractor elects to continue to perform all of its obligations under this Agreement, or (b) if not delivered under (a) above, upon rejection of this Agreement by or on behalf of Contractor upon written request therefore by City. If, in a bankruptcy or insolvency proceeding involving Contractor, the provisions of the U.S. Bankruptcy Code referenced above are determined not to apply, City shall nevertheless be entitled to no less than the protection offered by the provisions of the U.S. Bankruptcy Code with respect to its entitlement to and rights to the use and possession of all intellectual property to which City has been granted rights under this Agreement notwithstanding the bankruptcy or insolvency of Contractor.

21. Assignment

Contractor shall not assign or otherwise transfer any rights, duties, obligations or interest in this Agreement or arising hereunder to any person, persons, entity or entities whatsoever without the prior written consent of the City and any attempt to assign or transfer without such prior written consent shall be void. Consent to any single assignment or transfer shall not constitute consent to any further assignment or transfer. In the event that Contractor assigns this Agreement in compliance with this provision, this Agreement and all of its provisions shall inure to the benefit of and become binding upon the parties and the successors and permitted assigns of the respective parties.

22. Agents/Brokers

Contractor warrants that Contractor has not employed or retained any subcontractor, agent, company or person other than bona fide, full-time employees of Contractor working solely for Contractor, to solicit or secure this Agreement, and that Contractor has not paid or agreed to pay any subcontractor, agent, company or persons other than bona fide employees any fee, commission, percentage, gifts or any other consideration, contingent upon or resulting from the award of this Agreement. For breach or violation of this warranty, the City shall have the right to rescind this Agreement without liability or, in its discretion, to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such fee, commission, percentage or gift.

23. Publicity

Any publicity generated by Contractor for the project funded pursuant to this Agreement, during the term of this Agreement or for one year thereafter, will make reference to the contribution of the City of Oakland in making the project possible. The words "City of Oakland" will be

explicitly stated in all pieces of publicity, including but not limited to flyers, press releases, posters, brochures, public service announcements, interviews and newspaper articles.

City staff will be available whenever possible at the request of Contractor to assist Contractor in generating publicity for the project funded pursuant to this Agreement. Contractor further agrees to cooperate with authorized City officials and staff in any City-generated publicity or promotional activities undertaken with respect to this project.

24. Conflict of Interest

(a) Contractor

The following protections against conflict of interest will be upheld:

(1) Contractor certifies that no member of, or delegate to the Congress of the United States shall be permitted to share or take part in this Agreement or in any benefit arising there from.

(2) Contractor certifies that no member, officer, or employee of the City or its designees or agents, and no other public official of the City who exercises any functions or responsibilities with respect to the programs or projects covered by this Agreement, shall have any interest, direct or indirect in this Agreement, or in its proceeds during his/her tenure or for one year thereafter.

(3) Contractor shall immediately notify the City of any real or possible conflict of interest between work performed for the City and for other clients served by Contractor.

(4) Contractor warrants and represents, to the best of its present knowledge, that no public official or employee of City who has been involved in the making of this Agreement, or who is a member of a City board or commission which has been involved in the making of this Agreement whether in an advisory or decision-making capacity, has or will receive a direct or indirect financial interest in this Agreement in violation of the rules contained in California Government Code Section 1090 et seq., pertaining to conflicts of interest in public contracting. Contractor shall exercise due diligence to ensure that no such official will receive such an interest.

(5) Contractor further warrants and represents, to the best of its present knowledge and excepting any written disclosures as to these matter already made by Contractor to City, that (1) no public official of City who has participated in decision-making concerning this Agreement or has used his or her official position to influence decisions regarding this

Agreement, has an economic interest in Contractor or this Agreement, and (2) this Agreement will not have a direct or indirect financial effect on said official, the official's spouse or dependent children, or any of the official's economic interests. For purposes of this paragraph, an official is deemed to have an "economic interest" in any (a) for-profit business entity in which the official has a direct or indirect investment worth $2,000 or more, (b) any real property in which the official has a direct or indirect interest worth $2,000 or more, (c) any for-profit business entity in which the official is a director, officer, partner, trustee, employee or manager, or (d) any source of income or donors of gifts to the official (including nonprofit entities) if the income totaled more than $500 in the previous 12 months, or value of the gift totaled more than $350 the previous year. Contractor agrees to promptly disclose to City in writing any information it may receive concerning any such potential conflict of interest. Contractor's attention is directed to the conflict of interest rules applicable to governmental decision-making contained in the Political Reform Act (California Government Code Section 87100 et seq.) and its implementing regulations (California Code of Regulations, Title 2, Section 18700 et seq.).

(6) Contractor understands that in some cases Contractor or persons associated with Contractor may be deemed a "City officer" or "public official" for purposes of the conflict of interest provisions of Government Code Section 1090 and/or the Political Reform Act. Contractor further understands that, as a public officer or official, Contractor or persons associated with Contractor may be disqualified from future City contracts to the extent that Contractor is involved in any aspect of the making of that future contract (including preparing plans and specifications or performing design work or feasibility studies for that contract) through its work under this Agreement.

(7) Contractor shall incorporate or cause to be incorporated into all subcontracts for work to be performed under this Agreement a provision governing conflict of interest in substantially the same form set forth herein.

(b) No Waiver

Nothing herein is intended to waive any applicable federal, state or local conflict of interest law or regulation.

(c) Remedies and Sanctions

In addition to the rights and remedies otherwise available to the City under this Agreement and under federal, state and local law, Contractor understands and agrees that, if the City reasonably determines that Contractor has failed to make

a good faith effort to avoid an improper conflict of interest situation or is responsible for the conflict situation, the City may (1) suspend payments under this Agreement, (2) terminate this Agreement, (3) require reimbursement by Contractor to the City of any amounts disbursed under this Agreement. In addition, the City may suspend payments or terminate this Agreement whether or not Contractor is responsible for the conflict of interest situation.

25. Validity of Contracts

The Oakland City Council must approve all Agreements greater than $15,000. This Agreement shall not be binding or of any force or effect until signed by the City Manager or his or her designee and approved as to form and legality by the City Attorney or his or her designee.

26. Governing Law

This Agreement shall be governed and construed in accordance with the laws of the State of California, without reference to its conflicts of laws principles. Any action or proceeding to enforce the terms of this Agreement shall be brought in the courts of Alameda County, Oakland, California and each party agrees to waive any objections to personal jurisdiction and venue in the courts of Alameda County, Oakland, California.

27. Headings

Headings and captions used to introduce Sections and paragraphs of this Agreement are for convenience, only, and have no legal significance.

28. Construction

(a) Except as provided in Section 12 (b) above, acceptance or acquiescence in a prior course of dealing or a course of performance rendered under this Agreement or under any Change Order, or Change Notice, shall not be relevant in determining the meaning of this Agreement even though the accepting or acquiescing party has knowledge of the nature of the performance and opportunity for objection.

(b) The language in all parts of this Agreement and any Purchase Order, Change Order, or Change Notice, shall in all cases be construed in whole, according to its fair meaning, and not strictly for or against, either Contractor, City regardless of the drafter of such part.

28. Waiver

No covenant, term, or condition of this Agreement may be waived except by written consent of the party against whom the waiver is claimed and the waiver of any term, covenant or condition of this Agreement shall not be deemed a waiver of any subsequent breach of the same or any other term, covenant or condition of this Agreement.

30. Independent Contractor

(a) Rights and Responsibilities

It is expressly agreed that in the performance of the services necessary to carry out this Agreement, Contractor shall be, and is, an independent contractor, and is not an employee of the City. Contractor acknowledges and agrees that all of Contractor's employees and subcontractors are under the sole direction and control of Contractor and City shall have no authority over or responsibility for such employees and subcontractors of Contractor. Contractor has and shall retain the right to exercise sole direction and supervision of the services, and full control over the employment, direction, compensation and discharge of all persons assisting Contractor in the performance of Contractor's services hereunder. Contractor shall be solely responsible for all matters relating to the payment of his/her employees, including compliance with social security, withholding and all other regulations governing such matters, and shall be solely responsible for Contractor's own acts and those of Contractor's subordinates and employees. Contractor will determine the method, details and means of performing the services described in **EXHIBIT 1/Schedule A.**

(b) Contractor's Qualifications

Contractor represents that Contractor has the qualifications and skills necessary to perform the services under this Agreement in a competent and professional manner without the advice or direction of the City. This means Contractor is able to fulfill the requirements of this Agreement. Failure to perform all of the services required under this Agreement will constitute a material breach of the Agreement and may be cause for termination of the Agreement. Contractor has complete and sole discretion for the manner in which the work under this Agreement is performed. Contractor shall complete and submit to City, Schedule M-Independent Contractor Questionnaire, prior to the execution of this Agreement.

(c) Payment of Income Taxes

Contractor is responsible for paying, when due, all income taxes, including estimated taxes, incurred as a result of the compensation paid by the City to Contractor for services under this Agreement. On request, Contractor will provide the City with proof of timely payment. Contractor agrees to indemnify the City

for any claims, costs, losses, fees, penalties, interest or damages suffered by the City resulting from Contractor's failure to comply with this provision.

(d) Non-Exclusive Relationship

Contractor may perform services for, and contract with, as many additional clients, persons or companies as Contractor, in his or her sole discretion, sees fit.

(e) Tools, Materials and Equipment

Contractor will supply all tools, except those tools, materials, equipment specified herein, if any, required to perform the services under this Agreement.

(f) Cooperation of the City

The City agrees to comply with all reasonable requests of Contractor necessary to the performance of Contractor's duties under this Agreement.

(g) Extra Work

Contractor will do no extra work under this Agreement without first receiving prior written authorization from the City.

31. Attorneys' Fees

If either party commences an action or proceeding to determine or enforce its rights hereunder, the prevailing party shall be entitled to recover from the losing party all expenses reasonably incurred, including court costs, reasonable attorneys' fees and costs of suit as determined by the court.

32. Counterparts

This Agreement may be executed in any number of identical counterparts, any set of which signed by both parties shall be deemed to constitute a complete, executed original for all purposes.

33. Remedies Cumulative

The rights and remedies of City provided in this Agreement shall not be exclusive and are in addition to any other rights and remedies provided by law, including the California Uniform Commercial Code.

34. Severability/Partial Invalidity

If any term or provision of this Agreement, or the application of any term or provision of this Agreement to a particular situation, shall be finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then notwithstanding such determination, such term or provision shall remain in force and effect to the extent allowed by such ruling and all other terms and provisions of this Agreement or the application of this Agreement to other situation shall remain in full force and effect.

Notwithstanding the foregoing, if any material term or provision of this Agreement or the application of such material term or condition to a particular situation is finally found to be void, invalid, illegal or unenforceable by a court of competent jurisdiction, then the Parties hereto agree to work in good faith and fully cooperate with each other to amend this Agreement to carry out its intent.

35. Access

Access to City's premises by Contractor shall be subject to the reasonable security and operational requirements of City. To the extent that Contractor's obligations under this Agreement or any Purchase Order, Change Order, or Change Notice, require the performance of Services or Work by Contractor on City's property or property under City's control, Contractor agrees:

(i) to accept full responsibility for performing all Services or work in a safe manner so as not to jeopardize the safety of City's personnel, property, or members of the general public; and

(ii) to comply with and enforce all of City's regulations, policies, and procedures including, without limitation, those with respect to security, access, safety and fire protection, City's policy against sexual harassment, and all applicable state and municipal safety regulations, building codes or ordinances.

36. Entire Agreement of the Parties

This Agreement supersedes any and all Agreements, either oral or written, between the parties with respect to the rendering of services by Contractor for the City and contains all of the representations, covenants and Agreements between the parties with respect to the rendering of those services. Each party to this Agreement acknowledges that no representations, inducements, promises or Agreements, orally or otherwise, have been made by any party, or anyone acting on

behalf of any party, which are not contained in this Agreement, and that no other Agreement, statement or promise not contained in this Agreement will be valid or binding.

37. Modification

Any modification of this Agreement will be effective only if it is in a writing signed by all parties to this Agreement.

38. Notices

If either party shall desire or be required to give notice to the other, such notice shall be given in writing, via facsimile and concurrently by prepaid U.S. certified or registered postage, addressed to recipient as follows:

(City of Oakland)
Oakland Police Department
455 7th Street
Oakland, CA 94607
Attn: Capt Roland Holmgren, *or his Designee*

cc:
Tricia Hynes, *or her Designee*
Deputy City Attorney
1 Frank Ogawa Plaza, 6th Fl.
Oakland, CA 94612

(Contractor)
Forensic Logic LLC
712 Bancroft Road #423
Walnut Creek, CA 94598
Attn: Robert L. Batty

Any party to this Agreement may change the name or address of representatives for purpose of this Notice paragraph by providing written notice to all other parties ten (10) business days before the change is effective.

39. Right to Offset

All claims for money or to become due from City shall be subject to deduction or offset by City from any monies due Contractor by reason of any claim or counterclaim arising out of this Agreement or any Purchase Order, Change Order, or Change Notice or any other transaction with Contractor. To the extent that there are amounts due to the City and to a state or federal funding agency, and the amount of the offset is insufficient to pay such amount in full, the amount of the offset shall be prorated between the City and such state or federal funding agency in proportion to the amounts due them.

40. No Third Party Beneficiary

This Agreement shall not be construed to be an agreement for the benefit of any third Party or parties, and no third party or parties shall have any claim or right of action under this Agreement

41. Survival

Sections (2, 7, 8, 9, 10, 14, 15, 17, 26 and 40) of this Agreement, along with any other provisions which by their terms survive, shall survive the expiration or termination of this Agreement.

42. Time is of the Essence

The Special Circumstances of this Agreement require Contractor's timely performance of its obligations under this Agreement. Therefore, time is of the essence in the performance of this Agreement.

43. Authority

Each individual executing this Agreement or any Purchase Order, Change Order or Change Notice, hereby represents and warrants that he or she has the full power and authority to execute this Agreement or such Purchase Order, Change Order or Change Notice, on behalf of the named party such individual purports to bind.

SO AGREED:

City of Oakland,
a municipal corporation

Deborah Barnes 10/02/18
(City Administrator's Office) (Date)

Contractor Forensic Logic LLC

[signature] 9/16/2018
(Signature) (Date)

[signature] 10/1/18
(Department Head Signature) (Date)
for Chief Kirkpatrick

Business Tax No. 00200554
(Business Tax Certificate No.)

Approved as to form and legality:

Brigid Hynes 9/27/18
(City Attorney's Office Signature) (Date)

RESOLUTION 87193 C.M.S.
(Resolution Number)

ATTACHMENT B

Schedule Q
INSURANCE REQUIREMENTS
IT Professional/Cyber Liability Exposures
(Revised 1/13/2017:dkg)

a. General Liability, Automobile, Workers' Compensation and Professional Liability

Contractor shall procure, prior to commencement of service, and keep in force for the term of this contract, at Contractor's own cost and expense, the following policies of insurance or certificates or binders as necessary to represent that coverage as specified below is in place with companies doing business in California and acceptable to the City. If requested, Contractor shall provide the City with copies of all insurance policies. The insurance shall at a minimum include:

i. **Commercial General Liability insurance** shall cover bodily injury, property damage and personal injury liability for premises operations, independent contractors, products-completed operations personal & advertising injury and contractual liability. Coverage shall be at least as broad as Insurance Services Office Commercial General Liability coverage (occurrence Form CG 00 01)

Limits of liability: Contractor shall maintain commercial general liability (CGL) and, if necessary, commercial umbrella insurance with a limit of not less than $2,000,000 each occurrence. If such CGL insurance contains a general aggregate limit, either the general aggregate limit shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit.

ii. **Automobile Liability Insurance.** Contractor shall maintain automobile liability insurance for bodily injury and property damage liability with a limit of not less than $1,000,000 each accident. Such insurance shall cover liability arising out of any auto (including owned, hired, and non-owned autos). Coverage shall be at least as broad as Insurance Services Office Form Number CA 0001.

iii. **Worker's Compensation insurance** as required by the laws of the State of California, with statutory limits, and statutory coverage may include Employers' Liability coverage, with limits not less than $1,000,000 each accident, $1,000,000 policy limit bodily injury by disease, and $1,000,000 each employee bodily injury by disease. The Contractor certifies that he/she is aware of the provisions of section 3700 of the California Labor Code, which requires every employer to provide Workers' Compensation coverage, or to undertake self-insurance in accordance with the provisions of that Code. The Contractor shall comply with the provisions of section 3700 of the California Labor Code before commencing performance of the work under this Agreement and thereafter as required by that code.

iv. ***Technology Professional Liability*** *(Errors and Omissions) OR* ***Cyber Liability Insurance*** *appropriate to the Consultant's profession, with limits not less than* ***$2,000,000*** *per occurrence or claim,* ***$2,000,000*** *aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Consultant in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.*

b. Terms Conditions and Endorsements

The aforementioned insurance shall be endorsed and have all the following conditions:

i. Insured Status (Additional Insured): Contractor shall provide insured status naming the City of Oakland, its Councilmembers, directors, officers, agents, employees and volunteers as insured's under the Commercial General Liability policy. General liability coverage can be provided in the form of an endorsement to the Consultant's insurance (at least as broad as ISO Form CG 20 10 11 85 or **both** CG 20 10, CG 20 26, CG 20 33, or CG 20 38; **and** CG 20 37 forms if later revisions used). A STATEMENT OF ADDITIONAL INSURED STATUS ON THE ACORD INSURANCE CERTIFICATE FORM IS INSUFFICIENT AND WILL BE REJECTED AS PROOF OF MEETING THIS REQUIREMENT; and

ii. Coverage afforded on behalf of the City, Councilmembers, directors, officers, agents, employees and volunteers shall be primary insurance. Any other insurance available to the City Councilmembers, directors, officers, agents, employees and volunteers under any other policies shall be excess insurance (over the insurance required by this Agreement); and

iii. Cancellation Notice: Each insurance policy required by this clause shall provide that coverage shall not be canceled, except with notice to the Entity; and

iv. Certificate holder is to be the same person and address as indicated in the "Notices" section of this Agreement; and

v. Insurer shall carry insurance from admitted companies with an A.M. Best Rating of A:VII, or better.

c. Replacement of Coverage

In the case of the breach of any of the insurance provisions of this Agreement, the City may, at the City's option, take out and maintain at the expense of Contractor, such

insurance in the name of Contractor as is required pursuant to this Agreement, and may deduct the cost of taking out and maintaining such insurance from any sums which may be found or become due to Contractor under this Agreement.

d. Insurance Interpretation

All endorsements, certificates, forms, coverage and limits of liability referred to herein shall have the meaning given such terms by the Insurance Services Office as of the date of this Agreement.

e. Proof of Insurance

Contractor will be required to provide proof of all insurance required for the work prior to execution of the contract, including copies of Contractor's insurance policies if and when requested. Failure to provide the insurance proof requested or failure to do so in a timely manner shall constitute ground for rescission of the contract award.

f. Subcontractors

Should the Contractor subcontract out the work required under this agreement, they shall include all subcontractors as insured's under its policies or shall maintain separate certificates and endorsements for each subcontractor. As an alternative, the Contractor may require all subcontractors to provide at their own expense evidence of all the required coverages listed in this Schedule. If this option is exercised, both the City of Oakland and the Contractor shall be named as additional insured under the subcontractor's General Liability policy. All coverages for subcontractors shall be subject to all the requirements stated herein. The City reserves the right to perform an insurance audit during the course of the project to verify compliance with requirements.

g. Deductibles and Self-Insured Retentions

Any deductible or self-insured retention must be declared to and approved by the City. At the option of the City, either: the insurer shall reduce or eliminate such deductible or self-insured retentions as respects the City, its Councilmembers, directors, officers, agents, employees and volunteers; or the Contractor shall provide a financial guarantee satisfactory to the City guaranteeing payment of losses and related investigations, claim administration and defense expenses.

h. Waiver of Subrogation

Contractor waives all rights against the City of Oakland and its Councilmembers, officers, directors, employees and volunteers for recovery of damages to the extent these damages are covered by the forms of insurance coverage required above.

i. Evaluation of Adequacy of Coverage

The City of Oakland maintains the right to, acting reasonably, modify, delete, alter or change these requirements, with reasonable notice, upon not less than ninety (90) days prior written notice.

j. Higher Limits of Insurance

If the contractor maintains higher limits than the minimums shown above, the City shall be entitled to coverage for the higher limits maintained by the contractor.

k. Claims Made Policies

If any of the required policies provide coverage on a claims-made basis:

1. The Retroactive Date must be shown and must be before the date of the contract or the beginning of contract work.

2. Insurance must be maintained and evidence of insurance must be provided ***for at least five (5) years after completion of the contract of work.***

3. If coverage is canceled or non-renewed, and not ***replaced with another claims-made policy form with a Retroactive Date*** prior to the contract effective date, the Consultant must purchase "extended reporting" coverage for a minimum of ***five (5)*** years after completion of contract work.

END OF SCHEDULE Q – INSURANCE REQUIREMENT