CITY OF OAKLAND

Privacy Advisory Commission

April 5, 2018 5:00 PM

Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd Floor

Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Clint M. Johnson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Saied R. Karamooz, **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. 5:00pm: Call to Order, determination of quorum

2. 5:05pm: Review and approval of February meeting minutes

3. 5:10pm: Open Forum

4. 5:15pm: Introduction of new commissioners

5. 5:20pm: Presentation by UC Berkeley School of Information – CRIMS Privacy Assessment. Possible Action – Accept report; make recommendations to the City Council.

6. 5:45pm: Review and take possible action on Sanctuary City Contracting Ordinance

7. 5:55pm: Review and take possible action on Cell Site Simulator Annual Report

8. 6:10pm: Community Inquiry into Landlord Tax Audit/Business Revenue Data Requests (presentation by Strauss, Keenan). Possible Action – make recommendations to the City Council.

9. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

February 1, 2018 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 3rd Floor
Meeting Minutes

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Vacant, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Clint M. Johnson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Saied R. Karamooz, **Mayoral Representative**: Vacant*

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. 5:00pm: Call to Order, determination of quorum

The meeting was called to order at 6:05; members present: Hofer, Johnson, Jaquez, Katz, Karamooz, Oliver.

2. 5:05pm: Review and approval of November and January meeting minutes

The November and January Minutes were approved unanimously.

3. 5:10pm: Open Forum
4.

There were no public speakers.

5. 5:15pm: Presentation by Oakland Police Department - Annual Report on Cellular Site Simulator Use

Chairperson Hofer introduced the report as a game changing moment in privacy rights in that it is the first known annual report from a City about this type of device. He noted the County also recently released its first annual report and that this is an example of good public policy.

Tim Birch reviewed the report's key elements. Noting that no recording of data occurred and there were no costs associated.

Member Jaquez asked about the cost of training for officers who use the device; Mr. Birch answered that the training was done in house and at no cost to the department but that any future training costs would be reported. Member Katz asked about the efficacy of the device based on the success rate listed in the report (1 out of 3 arrests). Chairperson Hofer added a little more detail would help in regard to whether it was the suspect or the phone that was located. Mr. Birch offered to get more details and add them to the report, bringing it back to the PAC before going to City Council.

6. 5:35pm: Presentation by Oakland Police Department - Private Video Camera Registry

Bruce Stoffmacher with OPD presented a PowerPoint about the program which is an online registry that private citizens can voluntarily use to register their camera with the police department. He demonstrated the website and explained the protocols in place to avoid any release of people's personal information. He also explained that this does NOT give OPD live access to any private camera but merely tells officers where they are located so that they could approach camera owners after-the-fact when investigating a crime. This will save countless hours of time for investigators because they will be aware of where cameras are located without having to conduct door-to-door canvassing.

Some questions arose regarding data and he explained that all of the data is held internally and stored on OPD servers. Outside vendors were only used to develop the GIS mapping function. Only OPD staff with a certified email account will have access to the database.

Two Public Speakers:

Michael Katz-Lacabe raised some concerns about officers installing the application on their personal versus city-issued mobile devices' encryption of the data, and how a user's info is validated; noting that a hacker could distort the data in the system and add a bunch of non-existent cameras to confuse OPD.

J.P. Masser supported the concern about authentication raised by the previous speaker and raised a concern about how much footage an officer would collect from a particular camera.

7. 5:55pm: Annual election of Chair, Vice-Chair

Both Chairperson Hofer and Vice Chair Johnson were reelected unanimously.

8. Adjournment

The meeting adjourned at 5:45.

An Assessment of Potential Privacy Problems of the Consolidate Records Information Management System

Kimberly Fong, Peter Rowland, Steve Trush
UC Berkeley School of Information

Introduction.

On January 26, 2018, the City of Oakland passed Resolution No. 87036, reaffirming the City's status as a Sanctuary City and its commitment to protect undocumented persons fearful of discrimination, detention, and deportation. The Resolution established the City of Oakland's policy of refusing law enforcement assistance, even traffic support, to Immigration and Customs Enforcement (ICE) actions. In accordance with City policy, the Oakland Police Department's (OPD) Immigration Policy Manual 415 states that OPD "does not collect or maintain any information regarding a person's immigration status" unless used for completing U or T visa documents.[1] Furthermore, officers may respond to requests for information from immigration enforcement agencies only when the requests are accompanied by a judicial warrant.

City leaders now seek to determine whether OPD's information systems share data with agencies that might use the data to pursue immigration-related actions. One such system, the Consolidated Records Information Management System (CRIMS), shares criminal justice-related data with federal agencies, including the Department of Homeland Security (DHS); state agencies; and other law enforcement agencies within Alameda County.

For our work, we conducted a values-based investigation from a public citizen's perspective with limited access to the system and analyzed the potential privacy risks associated with citizenship-related data in CRIMS. We relied on the National Institute of Standards and Technology's (NIST) Privacy Risk Assessment Framework to guide our approach and frame our recommendations. Through interviews, content analysis, and system walkthroughs, we uncovered several potential risks to the privacy of citizenship-related data and offer recommendations to mitigate those risks.

System Description.

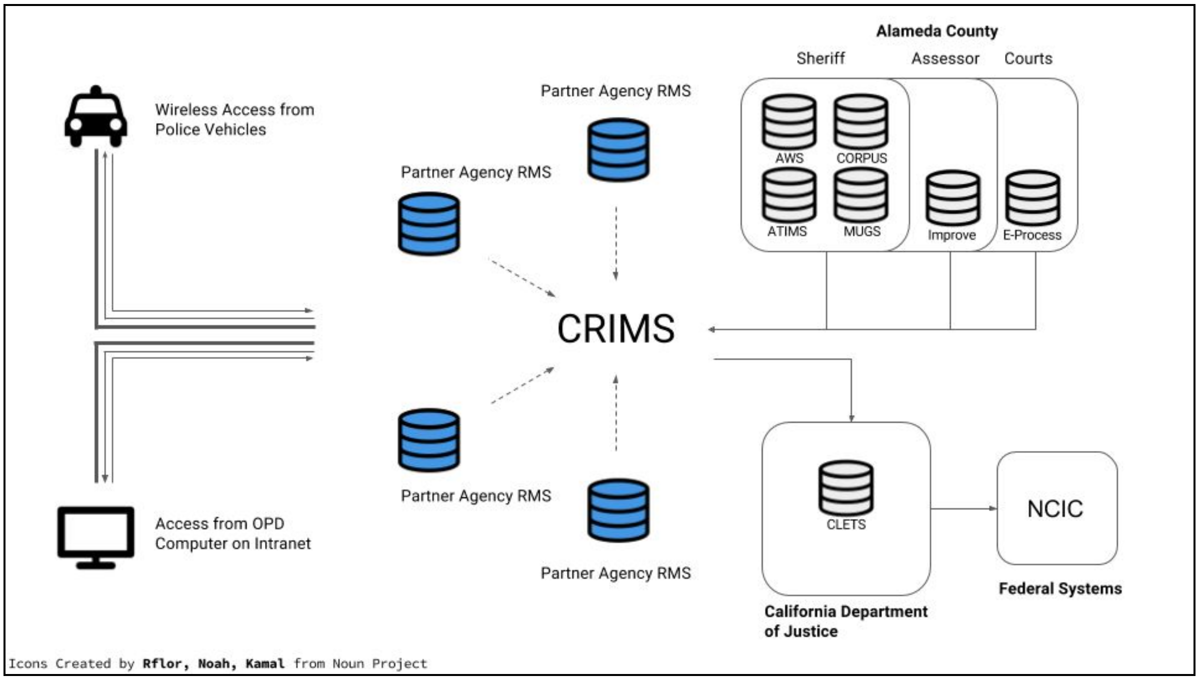
CRIMS is an online portal for law enforcement and criminal justice agencies within Alameda County. Alameda County Information Technology Department (AC ITD) maintains the system, and the Alameda County Sheriff governs it. CRIMS is accessible by eligible police departments within Alameda County, the Sheriff's Office, and the District Attorney of Alameda County, and it provides access to both police departments' local record management systems and the state-level information-sharing network, the California Law Enforcement Telecommunication System (CLETS). The California Department of Justice (CA DOJ) administers CLETS but delegates authority to the Alameda County Sheriff to provide access to CLETS to agencies within the county. Along with that delegation of authority, the Alameda County Sheriff must also ensure that connecting systems are compliant with CLETS security policies.[2]

CRIMS provides a centralized interface for participating agencies in Alameda County to access CLETS, and facilitates the filing of criminal and court records required by the CA DOJ through this interface.

[1] Oakland Police Department, Policy 415 Immigration, *available at* http://www2.oaklandnet.com/oakca1/groups/police/documents/webcontent/oak065136.pdf.

[2] California Department of Justice, CLETS Policies, Practices, and Procedures (2014): 10.

CLETS policies define specific responsibilities for the Alameda County Sheriff to log all traffic on its interface for a period of three years. System interactions must be logged in enough detail for that time frame to determine, for any traffic that went through the interface, whether or not it was delivered, when it was delivered, and the agency and device to which it was delivered.[3]



Icons Created by **Rflor, Noah, Kamal** from Noun Project

Participating Agencies Providing Access to RMS Data:

Alameda County Sheriff's Office
Berkeley PD
Hayward PD
Oakland PD
UC Berkeley PD

Alameda PD
Dublin PD
Livermore PD
Piedmont PD
Union City PD

BART (Bay Area Rapid Transit) PD
Fremont PD
Oakland Housing Authority
San Leandro PD

Additional Participating Agencies Listed in 2007 MOU (not confirmed to contribute RMS data):

Alameda County Probation Dept
Emeryville PD

Albany PD
Newark PD

East Bay Regional Park District PD
California State University East Bay PD

System Governance.

Local law enforcement agencies in Alameda County must sign a Memorandum of Understanding (MOU) to access CRIMS. Pursuant to the MOU, member agencies agree to share releasable information from their record management systems (RMS) with all of the other participating member agencies. Critically, the MOU also allows a separate oversight committee, the Criminal Justice Information and Management Systems Committee (CJIMS), to authorize full or limited access to CRIMS information to a non-member agency. CJIMS is co-chaired by the Alameda County Sheriff and the District attorney, with members appointed by the Board of Supervisors.

[3] *Id*. at 27.

CRIMS is subject to several layers of laws and policies at the city, state, and federal levels, some of which may be incompatible with the terms of the CRIMS MOU. At the city level, CRIMS is operated by OPD, which adopts and operates under OPD Policies and General Orders that must be facially consistent with the City's laws and policies. In particular, OPD Policy 415[4] asserts that "OPD does not collect or maintain any information regarding a person's immigration status, unless the information is gathered specifically for the purposes of completing U visa or T visa documents." In addition, the Policy prohibits OPD from sharing non-public information about an individual's address, upcoming court date, or release date with U.S. Immigration and Customs Enforcement or Customs and Border Protection.

At the county level, Alameda County Ordinance Nos. 9.36.010 and 9.36.020[5] criminalize unauthorized access and disclosure, respectively, of "personal data" from the county's criminal database.[6] At the state level, beyond the protections of California's constitutional right to privacy,[7] policies governing the California Law Enforcement Telecommunications System (CLETS)--the statewide law enforcement network--also apply to the county and its member cities. Specifically, the CLETS Policies, Practices, and Procedures[8] assert that access to the network is available on a "right-to-know" and "need-to-know" basis, and that the system may only be used for law enforcement purposes. Federal policies and regulations include, for example, the FBI's Information Security Policy,[9] policies generated by the Criminal Justice Information Services Division (CJIS), and regulations applicable to the National Crime Information Center (NCIC) data.

As of 2016, the Oakland City Council receives advice from the Oakland Privacy Advisory Commission (OPAC) regarding best practices and privacy goals for protecting citizens' privacy rights. Regulations that may not be directly applicable to CRIMS but that could include other OPD databases include the proposed Surveillance Equipment Ordinance.[10]

Problematic Data Actions.

Our analysis of CRIMS identified system actions that create privacy risks for data subjects. We estimate the probabilities of risks and their potential severity based on our understanding of the system because there is no objective standard for our measurements. Although we believe our estimates to be reasonably informed, we put forth that the strength of our analysis is not with risk probabilities per se, but rather with recognition of the relative importance of system characteristics for protecting or revealing sensitive information. It is important to note that these highlighted actions are not deliberate misuses of CRIMS, but risks arising out of expected uses of the system.

[4] Oakland Police Department, Policy 415 Immigration, *available at* http://www2.oaklandnet.com/oakca1/groups/police/documents/webcontent/oak065136.pdf.

[5] Alameda County Municipal Code §§ 9.36.010, 9.36.020.

[6] Although these ordinances explicitly apply to CRIMS's predecessor, the Criminal Oriented Records Production Unified System (CORPUS), it is arguable that they can or should be applicable to CRIMS..

[7] Cal. Const. art. I, § 1. ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.")

[8] CLETS Policies, Practices, and Procedures, *supra* n.1.

[9] Criminal Justice Information Services, CJIS Security Policy (2017), *available at* https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

[10] Oakland City Council, The Surveillance and Community Safety Ordinance (Draft), *available at* http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak062224.pdf.

Issue 1 - eProcess Submissions: Will OPD users be aware of whom data would be shared with or how it will be used when submitting arrest reports?

Details of Issue: Fields in the eProcess forms allow for the user to enter data that may indirectly disclose indications of person's citizenship status, including Place of Birth Location (a mandatory field to select one of 182 possible states, territories, or countries) or Place of Birth City (an optional field). Omissions may also indicate citizenship status, namely not including a Social Security Number (optional). Furthermore, according to OPD Policy 415 "Immigration", Section 6 "Information Sharing", an OPD officer "shall not share non-public information about an individual's address, upcoming court date, or release date with ICE or CBP." When filing a CAR, the user must enter the subject's Home Address (although a checkbox is present in case a subject refuses to provide the information); optionally, a user can enter the subject's Business Address. Users are instructed in Alameda County training manuals that a CAR is accessible to all law enforcement personnel and considered a public record.

Issue 1 Problematic Data Actions

1. Appropriation: Non-public addresses entered by OPD officers may be accessed by members of federal agencies (DHS) for immigration purposes despite the intentions of the OPD officer that filed the information.

2. Unanticipated Revelation: Contextual clues such as presence of Place of Birth information or absence of an SSN may provide indications of citizenship status of a person who has been arrested.

Issue 2 - eProcess Submissions: Will mandatory fields force OPD users to enter data that reveals citizenship status?

Details of Issue: As seen in Issue 1, CRIMS requires users to enter mandatory fields in order to submit eProcess forms. As such, mandatory data is requested that may violate OPD department policy ("non-public addresses") if accessed by federal organizations ICE or CBP. The design of the system is, however, determined by the Alameda County ITD. As the latest MOU for CRIMS states, "[e]ach Agency agrees to … System design recommendations as developed or modified by the Alameda County Information Technology Department (ITD)." It follows that the types of mandatory data requested can be determined by Alameda County without prior approval of the City of Oakland, although Alameda County ITD administrators expressed that all design changes would be made with input from participating agencies if Alameda County ITD determined that the change was relevant to that agency.

Issue 2 Problematic Data Actions

Induced Disclosure: Mandatory data fields regulate officer's data disclosure via the system architecture. As an officer cannot transfer a subject to the county jail without submitting a CAR, the officer is forced to disclose mandatory information about the individual. A subject can invoke right to silence, but the officer is expected to enter information if known.

Issue 3 - Person/Vehicle/Location Queries: Will personal information in OPD's RMS be unintentionally disclosed to other CRIMS users?

Details of Issue: According to the CRIMS MOU and confirmed via interview with Alameda County ITD office, participating agencies will "share their Agency's eligible RMS data as deemed releasable by individual agency guidelines." According to Alameda County ITD, participating agencies can set "SQL query"-like parameters for which data are released by the agency's RMS to be included in a CRIMS query. Misconfiguration or lack of awareness whether the current sharing configuration for personal information is in accordance with the department and the City of Oakland's policies could lead to data being unintentionally shared with CRIMS users.

Issue 3 Problematic Data Actions

Unanticipated Revelation: How personal information from OPD's RMS might be unintentionally shared with other CRIMS users would require further analysis of the RMS and its configuration for releasing data to CRIMS.

Issue 4 - Person/Vehicle/Location Queries: Will users assume access to query functions are restricted from federal agencies?
Details of Issue: According to the CRIMS MOU, "[f]ull or limited access to CRIMS information may be granted to other agencies. Requests for access will be reviewed by a CJIMS Committee to include the Alameda County Sheriff, the Alameda County District Attorney and the Alameda County Information Technology Department Manager. This group will determine what level of access, if any, is appropriate." Furthermore, in an email from Manu Shukla, the Alameda County ITD Criminal Justice manager, "State and federal agencies generally do not have access to RMS databases. The security granularity allows access to be granted to the Person/Vehicle / Location query tabs as well as separately to each of the different types of databases." As exceptions and increases to level of access can be made at the determination of the CJIMS without notification to the participating agencies, it is possible participating agencies may share data from their RMS under the assumption that any data shared from the RMS with CRIMS would not be shared with federal agencies.
Issue 4 Problematic Data Actions
Appropriation / Unanticipated Revelation: The use of information not intended for disclosure by OPD may possibly reveal non-public addresses or indicators of citizenship to federal agencies.

Issue 5 - Person/Vehicle/Location Queries: Will users rely on or be unable to correct incorrect data?
Details of Issue: It is unclear from our view of the query function whether it facilitates a user's ability to correct erroneous information uncovered in queries (if an inaccuracy is determined through questioning of a subject or other investigations) or how often a user would even perform those remedies if available. Unlike the eProcess functions that allows for forms to be updated by a submitting, arresting, or transporting officer until an arrestee is released from jail or up to 4 hours before the arrestee's first court appearance, query results likely require a user to contact a participating agency and having them correct their RMS. Furthermore, like many criminal justice databases, data subjects would not be offered the ability to see what information the databases contains and thus may not appeal any inaccurate data provided to the users.
Issue 5 Problematic Data Actions
Distortion: The use of inaccurate or misleading personal information could cause unjust actions against an individual. While not attributed to CRIMS, erroneous data within the Odyssey System used by Alameda County Courthouse led to extended jail stays and false arrests in 2016.

Recommendations.

Technical Recommendations.

1. **The City of Oakland should collaborate with Alameda County to create a mechanism for the regular reporting on outside agency access rights and use of data from CRIMS.** The City of Oakland should work with Alameda County to develop requirements for regular reporting on agency access rights, the frequency of use, and reasons for use for data within CRIMS. Specifically, if the granularity of logging allows it, OPD should be able to view these specifics with regards to OPD-collected data on individuals in Oakland. This reporting could possibly be a monthly report generated by Alameda County or accessed via the Reports tab of CRIMS.

2. **The City should assess and configure OPD's Record Management System to ensure compliance with city's Sanctuary City values and OPD's Policy 415 (Immigration).** We do not understand the link between OPD's RMS and CRIMS in terms of data shared by OPD's

system to CRIMS users. The assessment of the OPD's RMS was outside the scope of this project but is necessary to perform if one wants to completely understand how CRIMS might enable the disclosure of personal information. Once the relationship between RMS and CRIMS is examined and possible risks identified, the categories of data that are released from OPD can be technically controlled through system configuration.

CRIMS-specific Policy Recommendations.

3. **The City should review whether the submission of officer-collected data, specifically address, place of birth, and Social Security Number (SSN), via CRIMS eProcess forms is consistent with OPD Policy 415.** Contextual information such as place of birth or social security numbers may indicate a resident's citizenship status to other CRIMS users and required home address information may not be public information. As the system does not allow OPD to ensure that the information will not be received by DHS ICE or CBP, the City should review how users can feasibly minimize the inclusion of this data, including how officers ensure whether or not an address is already public information.

4. **The City should review and approve an updated CRIMS MOU to include notification of changes in system design and access rights of outside agencies.** Specifically, elected city officials should decide whether they concur with complete delegation of access control to the Alameda County CJIMS without input from participating agencies. The City should also determine what degree of notification from the County is sufficient upon system upgrade, re-design, or access right upgrades for outside agencies.

5. **Terms of CRIMS MOU should be limited to a set term and automatically require re-approval after significant changes to the system.** Other notable data sharing agreements, such as CLETS, are revisited periodically (e.g., every three years) to ensure that the conditions are agreed upon by all participating agencies. Additionally, if a system undergoes relevant changes such as the requirements of additional data, the MOU can include conditions that would require the City to re-approve the terms of the agreement.

Broader Policy Recommendations.

6. **The proposed Surveillance Ordinance should be amended to explicitly require City approval of data sharing agreements related to a department's surveillance technology use.** While the proposed ordinance would require approvals for surveillance use policies that includes a section on third-party data sharing, we feel that the approval of use policies that are governed by a separate data sharing agreement would require the City's approval of that governing document. As with the case of CRIMS, the Oakland Police Department's ability to control access and types of data disclosed is largely determined by Alameda County CJIMS; this delegation of responsibility to an outside entity could undermine even the most restrictive Surveillance Use Policy if functionality is modified or access is granted beyond what was originally considered in constructing the policy.

About This Report.

The authors of this report are Kimberly Fong, Peter Rowland, and Steve Trush, all graduate students at the UC Berkeley School of Information. Peter and Steve have been involved with the City of Oakland's Privacy Advisory Commission (OPAC) since the beginning of 2017 through a fellowship from the Center for Technology, Society, and Policy (CTSP). OPAC was formed in 2016 to provide citizen oversight and recommendations to the Oakland City Council about the use of surveillance technologies and privacy matters in the City of Oakland. As part of OPAC's mission to provide privacy guidance to city government, the commission is reviewing information systems used by the Oakland Police Department (OPD). We were originally asked to create a model for all of the systems used by OPD, and of its data-sharing with other agencies. The scope of this project was modified to analyze a single system, CRIMS, as a test case for privacy analysis that can be used for other information systems. We hope that this report will be useful for the Commission, as well as a model for how reports on other information systems can be produced. The primary audience for this report is the Commission, and we therefore recognize that our analysis and recommendations focused on Oakland, but apply by any CRIMS member agency.

Methodology.

We applied the NIST Privacy Risk Assessment Methodology[11] framework to evaluate CRIMS because NIST's framework is designed to identify concrete potential problems for individuals - such as loss of trust or self determination, discrimination, or economic loss - that may be caused during the processing of personally identifiable information (PII). The NIST framework - meant to be measurable and repeatable - introduces "privacy engineering" as a practical way of applying engineering practices to improving privacy risk management and facilitates the assessment of privacy-related risks and potential organizational impacts of an information system as well as the development of suitable controls for those risks. To gain the insight into the system design and gather information for completing the NIST framework, we leaned upon two models: Helen Nissenbaum's values in design framework for conceptualizing the meaning of values,[12] and Katie Shilton et al.'s methods for studying values dimensions.[13] Nissenbaum's framework presents an iterative process for examining the meaning of privacy in each of three modes: technical, philosophical, and empirical.

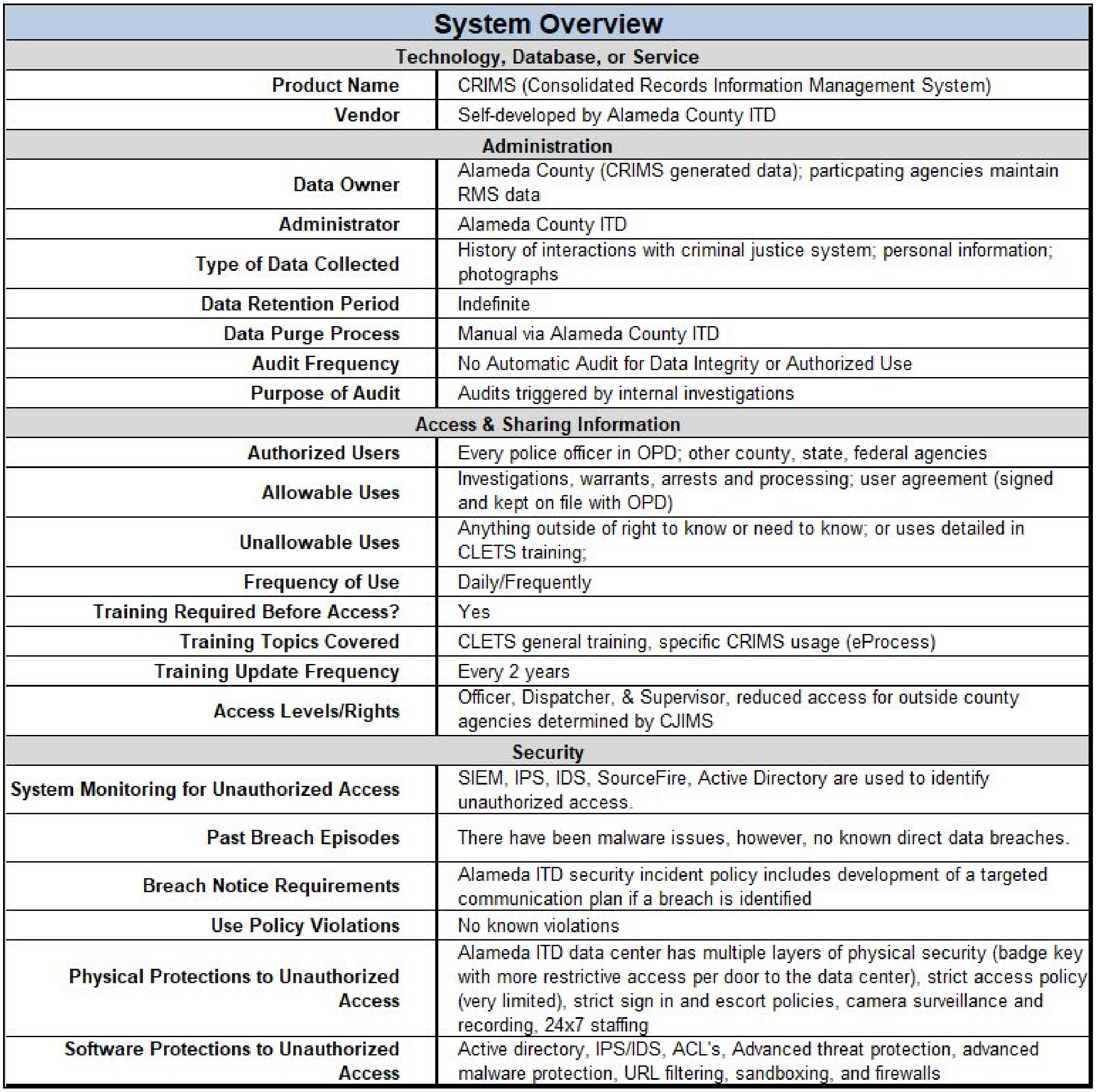
To read our full report, please visit:
http://people.ischool.berkeley.edu/~strush/CRIMS_FongRowlandTrush_Feb2018.pdf

[11] National Institute of Standards and Technology, NIST.IR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems (2017), *available at* http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[12] Helen Nissenbaum, "Values in technical design." *Encyclopedia of Science, Technology, and Ethics* (2005): 66-70.

[13] Katie Shilton, Jes A. Koepfler, and Kenneth R. Fleischmann, "How to see values in social computing: methods for studying values dimensions," *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing* (ACM 2014).

Appendix A - System Overview



System Overview	
Technology, Database, or Service	
Product Name	CRIMS (Consolidated Records Information Management System)
Vendor	Self-developed by Alameda County ITD
Administration	
Data Owner	Alameda County (CRIMS generated data); particpating agencies maintain RMS data
Administrator	Alameda County ITD
Type of Data Collected	History of interactions with criminal justice system; personal information; photographs
Data Retention Period	Indefinite
Data Purge Process	Manual via Alameda County ITD
Audit Frequency	No Automatic Audit for Data Integrity or Authorized Use
Purpose of Audit	Audits triggered by internal investigations
Access & Sharing Information	
Authorized Users	Every police officer in OPD; other county, state, federal agencies
Allowable Uses	Investigations, warrants, arrests and processing; user agreement (signed and kept on file with OPD)
Unallowable Uses	Anything outside of right to know or need to know; or uses detailed in CLETS training;
Frequency of Use	Daily/Frequently
Training Required Before Access?	Yes
Training Topics Covered	CLETS general training, specific CRIMS usage (eProcess)
Training Update Frequency	Every 2 years
Access Levels/Rights	Officer, Dispatcher, & Supervisor, reduced access for outside county agencies determined by CJIMS
Security	
System Monitoring for Unauthorized Access	SIEM, IPS, IDS, SourceFire, Active Directory are used to identify unauthorized access.
Past Breach Episodes	There have been malware issues, however, no known direct data breaches.
Breach Notice Requirements	Alameda ITD security incident policy includes development of a targeted communication plan if a breach is identified
Use Policy Violations	No known violations
Physical Protections to Unauthorized Access	Alameda ITD data center has multiple layers of physical security (badge key with more restrictive access per door to the data center), strict access policy (very limited), strict sign in and escort policies, camera surveillance and recording, 24x7 staffing
Software Protections to Unauthorized Access	Active directory, IPS/IDS, ACL's, Advanced threat protection, advanced malware protection, URL filtering, sandboxing, and firewalls

THE SANCTUARY CITY CONTRACTING AND INVESTMENT ORDINANCE

Whereas, President Trump issued an Executive Order on January 25, 2017 titled "Border Security and Immigration Enforcement" and created heightened fear and insecurity among many immigrant communities in Oakland and across the nation; and

Whereas, the City Council finds that the City of Oakland has a moral obligation to protect its residents from persecution; and

Whereas, the City Council finds that immigrants are valuable and essential members of both the California and Oakland community; and

Whereas, the City of Oakland has been on record since July 8, 1986 as a City of Refuge when it adopted Resolution No. 63950; and

Whereas, the City Council finds that a registry of individuals identified by religion, national origin, or ethnicity, in a list, database, or registry including that information, could be used by the government to persecute those individuals; and

Whereas, President Trump has repeatedly signaled that he intends to require Muslims to register in a database; and

Whereas, Trump advisors have invoked WWII Japanese-American internment as a precedent for the proposed expansion of the registry; and

Whereas, the Census Bureau turned over confidential information in 1943, including names and addresses, to help the US government identify Japanese Americans during World War II for the purpose of relocation; and

Whereas, President Trump has ordered a sweeping expansion of deportations and assigned unprecedented powers to Immigration and Customs Enforcement (ICE) officers targeting and terrorizing immigrant communities; and

Whereas, President Trump has issued three executive orders banning entry from certain Muslim-majority countries; and

Whereas, ICE Enforcement Removal Operations issued a Request for Information on August 3, 2017, to obtain commercial subscription data services capable of providing continuous real-time information pertaining to 500,000 identities per month from sources such as State Identification Numbers; real time jail booking data; credit history; insurance claims; phone number account information; wireless phone accounts; wire transfer data; driver's license information; Vehicle Registration Information; property information; pay day loan information; public court records; incarceration data; employment address data; Individual Taxpayer Identification Number (ITIN) data; and employer records; and

Whereas, ICE has a $1.6 million contract with Thomson-Reuters, maker of popular law firm software products such as WestLaw and PeopleMap, for the above services via its CLEAR software (Consolidated Lead Evaluation and Reporting); and

Whereas, ICE has proposed a $13.6 million four-year contract with Thomson-Reuters for continuing access to CLEAR that requires CLEAR to interface with Palantir's FALCON analytics, for the purposes of asset forfeiture investigations; and

Whereas, ICE has a $41 million contract with Palantir Technologies for the development of an intelligence system called Investigative Case Management, intended to be capable of providing information pertaining to an individual's schooling, family relationships, employment information, phone records, immigration history, foreign exchange program status, personal connections, biometric traits, criminal records, and home and work addresses; and

Whereas, the Department of Homeland Security published a new rule on September 18, 2017, authorizing the collection of social media information on all immigrants, including permanent residents and naturalized citizens; and

Whereas, ICE has awarded Giant Oak with $3 million for three separate contracts pertaining to social media data analytics services; and

Whereas, on September 8, 2017, ICE arrested hundreds of immigrants in intentionally targeted 'sanctuary' cities; and

Whereas, ICE's "Extreme Vetting Initiative" industry day attracted large corporations like IBM, Lexis-Nexis, SAS, Deloitte, Unisys, Booz Allen, SAIC, and Palantir in pursuit of contracts that would provide ICE with various data broker, social media threat modeling, and extreme vetting services; and

Whereas, on January 8, 2018, ICE awarded a contract to Vigilant to obtain access to Vigilant's commercially available license plate reader database, for the purpose of enhancing ICE's ability to pursue civil immigration violations; and

Whereas, IBM provided census tabulating card machines (Dehomag Hollerith D-11) and punch cards to Hitler's Third Reich, and custom-designed specialized applications at each major concentration camp throughout Germany and greater Europe enabling the Nazi Party to automate identification and persecution of Jews and others during the Holocaust; now therefore

THE CITY COUNCIL OF THE CITY OF OAKLAND DOES ORDAIN AS FOLLOWS:

Section 1. Title

This ordinance shall be known as the Sanctuary City Contracting and Investment Ordinance.

Section 2. Definitions

1) "City" means the City of Oakland, California.
2) "Data Broker" (also commonly called information broker, information reseller, data aggregator, and information solution provider) means either of the following:

   a. The collection of information, including personal information about consumers, from a wide variety of sources for the purposes of reselling such information to their customers, which include both private-sector businesses and government agencies;
   b. The aggregation of data that was collected for another purpose from that for which it is ultimately used.
3) "Extreme Vetting" means data-mining, threat modeling, predictive risk analysis, or other similar service.
4) "ICE" means the United States Immigration and Customs Enforcement, and any subdivision thereof.
5) "Person or Entity" means any natural person, corporation, institution, subsidiary, affiliate, or division under operating control of such person; the parent entities that have operating control over such person, and the subsidiaries, affiliates and divisions under operating control of such parent entity.

Section 3. Prohibition on Use of City Resources

1) No officer, employee, agent, department, board, commission, City Council, City Administrator, or other subdivision of the City shall enter into a new, amended, or extended contract or agreement with any Person or Entity that provides ICE with any "Data Broker" or "Extreme Vetting" services, as defined herein, unless the City Council makes a specific determination that no reasonable alternative exists, taking into consideration the following:
   a) The intent and purpose of this ordinance;
   b) The availability of alternative services, goods and equipment; and
   c) Quantifiable additional costs resulting from use of available alternatives.
2) All public works, construction bids, requests for information, requests for proposals, or any other solicitation issued by the City shall include notice of the prohibition listed above.
3) For the purpose of determining which person or entity provides ICE with Data Broker or Extreme Vetting services, the City Administrator shall rely on:
   a) Information published by reliable sources;
   b) Information released by public agencies;
   c) A declaration under the penalty of perjury executed by the Person or Entity, affirming that they do not provide Data Broker or Extreme Vetting services to ICE;
   d) Information submitted to the City Administrator by any member of the public, and thereafter duly verified.
4) Any Person or Entity identified as a supplier of Data Broker or Extreme Vetting services to ICE and potentially affected by this section shall be notified by the City Administrator of the determination. Any such Person or Entity shall be entitled to a review of the determination by appeal to the City Administrator. Request for such review shall be made within thirty (30) days of notification, or seven (7) days of the date of a City solicitation or notice of a pending contract or

purchase, of interest to the Person or Entity seeking review. Any Person or Entity vendor so identified may appeal the City Administrator's determination to the City Council, within fifteen (15) days of the determination.

5) Any existing contract, purchase agreement, or other obligation shall not be renewed or extended if the Person or Entity continues to provide Data Broker or Extreme Vetting services to ICE.

Section 4. Prohibition on Investment

1) The City of Oakland shall not make any investment in stocks, bonds, securities, or other obligations issued by any provider of Data Broker or Extreme Vetting services to ICE.
2) The City Council shall adopt a plan with respect to pension fund investments and shall implement such a plan consistent with the intent of this act.

Section 5. Investigation And Reporting

(a) The City Administrator, or his or her designee, shall review compliance with Sections 3-4. The City Administrator may initiate and shall receive and investigate all complaints regarding violations of Sections 3- 4. After investigating such complaints, the City Administrator shall issue findings regarding any alleged violation. If the City Administrator finds that a violation occurred, the City Administrator shall, within 30 days of such finding, send a report of such finding to the City Council, the Mayor, and the head of any department involved in the violation or in which the violation occurred. All officers, employees, departments, boards, commissions, and other entities of the City shall cooperate with the City Administrator in any investigation of a violation of Sections 3-4.

(b) The City Administrator shall coordinate with the City Attorney's office to remedy any such violations, and the City Attorney shall use all legal measures available to rescind, terminate, or void contracts awarded in violation of this ordinance.

(c) By April 1 of each year, each City department shall certify its compliance with this ordinance by written notice to the City Administrator. By May 1 of each year, the City Administrator shall submit to the Privacy Advisory Commission a written, public report regarding the department's compliance with Sections 3-4 over the previous calendar year. At minimum, this report must (1) detail with specificity the steps the department has taken to ensure compliance with Sections 3-4, (2) disclose any issues with compliance, including any violations or potential violations of this Ordinance, and (3) detail actions taken to cure any deficiencies with compliance. After receiving the recommendation of the Privacy Advisory Commission, if any, the City Administrator shall schedule and submit the written report to the City Council for review.

Section 6. Enforcement

(a) Cause of Action. Any violation of this Ordinance constitutes an injury, and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this Ordinance.

(b) Damages and Civil Penalties. If the City is found liable in a cause of action brought by an individual under section (a) above, the City shall be liable for (1) the damages suffered by the plaintiff, if any, as determined by the court, and (2) a civil penalty no greater than $5,000 per violation, as determined by the court. In determining the amount of the civil penalty, the court shall consider whether the violation was intentional or negligent, and any other prior violations of this ordinance by the City department that committed the violation.

(c) Attorney's Fees and Costs. A court shall award a plaintiff who prevails on a cause of action under subsection (a) reasonable attorney's fees and costs.

(d) Limitations on Actions. Any person bringing an action pursuant to this ordinance must first file a claim with the City pursuant to Government Code 905 or any successor statute within four years of the alleged violation.

(e) Any Person or Entity knowingly or willingly supplying false information in violation of Section 3 (3)(c), shall be guilty of a misdemeanor and up to a $1,000 fine.

Section 7. Severability

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

Section 8. Construction

The provisions of this Ordinance are to be construed broadly to effectuate the purposes of this Ordinance.

Section 9. Effective Date

This Ordinance shall take effect on [DATE].

CITY OF OAKLAND

MEMORANDUM

TO:	Anne Kirkpatrick Chief of Police	**FROM:**	Serge Babka Timothy Birch
SUBJECT:	Cellular Site Simulator – 2017 Annual Report	**DATE:**	January 23, 2018

Background

Oakland Police Department Lexipol Policy 609, Cellular Site Simulator Usage and Policy, requires that we provide an annual report. Section 609.7.2, Annual Report, requires that the “Cellular Site Simulator Program Coordinator shall provide the Chief of Police, the Privacy Advisory Commission, and Public Safety Committee with an annual report” that includes all of the below data points. (Sergeant Babka is currently the Program Coordinator.)

2017 Data Points

(a) The number of times cellular site simulator technology was requested: 3

(b) The number of times cellular site simulator technology was used: 3

(c) The number of times that agencies other than the Oakland Police Department received information from use of the equipment by the Oakland Police Department: OPD received information while operating the CSS with the DA Inspector. However, no data was downloaded, retained, or shared.

(d) The number of times the Oakland Police Department received information from use of this equipment by other agencies: OPD did not receive any data from use of this equipment by other agencies.

(e) Information concerning any violation of this policy including any alleged violations of policy. There were no policy violations.

(f) Total costs for maintenance, licensing and training, if any. OPD did not incur any maintenance, licensing, or training costs.

(g) The results of any internal audits and if any corrective action was taken, subject to laws governing confidentiality of employment actions and personnel rules. No audits were conducted due to low usage. All three deployments were reviewed and were in compliance with policy. No corrective action was needed.

(h) The number of times the equipment was deployed: 3

Additional Information

The below table provides additional information responsive to Policy section 609.7.1, Deployment Log, that is also required for the annual report.

Agency	Reason	Offense	Location	Results	Operators	Info Shared	Notes
Oakland PD	To make or attempt an arrest	187 PC (Murder)	Oakland Area 4	Unable to Locate	One OPD officer, two DA Inspectors	No	OPD Warrant
Other Agency (detail in notes)	To make or attempt an arrest	187 PC (Murder)	Hayward	Effected arrest	One OPD officer, two DA Inspectors	No	DA Inspector warrant. They requested one officer assist them in operating the device.
Other Agency (detail in notes)	To make or attempt an arrest	664/ 187 PC (Attempted Murder)	San Leandro	Unable to Locate	One OPD officer, two DA Inspectors	No	DA Inspector warrant. They requested one officer assist them in operating the device.

Respectfully submitted,

Serge Babka, Sergeant, Intelligence Unit
Timothy Birch, Police Services Manager I, Research and Planning