PUBLIC SAFETY COMMITTEE DISCUSSION AND ACTIONS

JULY 17, 2015

The meeting of the Public Safety Committee was called to order by Chair Terry Sinnott (North County Coastal) at 1:01 p.m. See the attached attendance sheet for Public Safety Committee member attendance.

1. APPROVAL OF MEETING MINUTES (APPROVE)

**Action:** Upon a motion by Councilmember Brian Bilbray (South County), and a second by Sheriff William D. Gore (San Diego County Sheriff), the Public Safety Committee approved its May 15, 2015, meeting minutes. Yes - Chair Sinnott, Vice Chair Steve Vaus (North County Inland), Councilmember Myrtle Cole (City of San Diego), Chief Jim Redman (County Chiefs'/Sheriff's Association-Seat A), Supervisor Greg Cox (County of San Diego), Chief Donald Butz (Regional Fire/Emergency Medical Services), Chief Adolfo Gonzales (San Diego County District Attorney's Office), Chief Shelley Zimmerman (San Diego Police Department), Sheriff Gore, and Councilmember Bilbray. No - None. Abstain - None. Absent - East County and County Chiefs'/Sheriff's Association, Seat B.

2. PUBLIC COMMENTS/COMMUNICATIONS/MEMBER COMMENTS

Chair Sinnott reported that Chief Bill Burke (Metropolitan Transit District) passed away on Monday, June 29, 2015.

A member of the public, Lorraine Leighton, made a public comment.

**REPORTS**

3. REPORT FROM CHIEFS'/SHERIFF'S MANAGEMENT COMMITTEE (INFORMATION)

Chief Redman reported on the July 1, 2015, meeting of the Chiefs'/Sheriff's Management Committee.

**Action:** This item was presented for information only.
4. **FY 2016 PROGRAM BUDGET AMENDMENT: JUVENILE MENTALLY ILL OFFENDER GRANT (APPROVE)**

Dr. Cynthia Burke (Director, Applied Policy/Criminal Justice Research), reported SANDAG was asked to be the research partner on a state grant for the County of San Diego Public Safety Group and Probation Department to increase mental health screening of youth entering the juvenile justice system and provide services to traumatized youth. **Action:** Upon a motion by Supervisor Cox, and a second by Councilmember Bilbray, the Public Safety Committee approved an amendment to the FY 2016 Program Budget to accept multi-year funding of $126,609 for the Juvenile Mentally Ill Offender Evaluation. Yes Chair Sinnott, Vice Chair Vaus, Councilmember Cole, Chief Redman, Supervisor Cox, Chief Butz, Chief Gonzales, Chief Zimmerman, Sheriff Gore, and Councilmember Bilbray. No - None. Abstain - None. Absent - East County and County Chiefs/Sheriff’s Association, Seat B.

5. **DRAFT AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM DATA SHARING MEMORANDUM OF UNDERSTANDING (DISCUSSION)**

Kurt Kroninger (Department Director, Technical Services) and Julie Wiley (Special Counsel) provided an update on the review process and proposed changes to the draft Memorandum of Understanding, which outlines the responsibilities of ARJIS and the law enforcement agencies that contribute to and access data from the ARJIS Enterprise. **Action:** This item was presented for discussion only.

6. **CRIME PREVENTION WITH NEXTDOOR.COM (INFORMATION)**

Officer Matthew Tortorella (San Diego Police Department) presented an overview of a partnership between the San Diego Police Department and Nextdoor.com as well as preliminary outcomes. The social networking service allows users to connect with people who live in their neighborhood. **Action:** This item was presented for information only.

7. **AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM DASHBOARD DEMONSTRATION (INFORMATION)**

Pamela Scanlon (Director, ARJIS) presented an overview of the Regional Mapping Dashboard that provides customized map views of the region to display various data such as sex offenders, crimes, and gangs. A demonstration of both the law-enforcement-only and the public dashboards was given. **Action:** This item was presented for information only.

8. **CONTINUED PUBLIC COMMENT**

None.
FACIAL RECOGNITION FAQs

How does facial recognition technology work?

Images of previously booked persons, along with identifying information are enrolled into a facial recognition database.

An automated process enrolls new mugshots daily, based on copies of the booking records that are transmitted from the Sheriff’s booking system.

A photo image of a person is obtained. This image is submitted via the mobile application. The backend process attempts to ‘match’ against existing mugshot photos by translating the image into a digital alphanumeric value (through a powerful algorithm) and find the closest values. Results are returned to the mobile application by confidence score (in reverse order). The officer then makes a visual judgment as to whether the person in the probe image is the same as the record on file.

What is the lawful purpose for utilizing facial recognition in the field?

Persons who are detained for offenses that warrant arrest and booking (lacking positive identification in the field) are subject to lawful identification requirements. Facial recognition saves time and in many cases allows for the release of detained persons without the need for the formal transportation to a booking facility.

From a Public Safety perspective, persons who are medically or mentally incapable of identifying themselves and who are a danger to themselves or others, or those who are deceased and not otherwise identified, are lawful candidates for facial recognition as a preliminary identification method.

Does the race, gender, hair style or hair color affect the results?

No. For each digital image, the algorithm makes measurements between the eyes, the tip of the nose and other strategic points within the facial structure and counts the pixels between them in order to assign the alphanumeric value to the image.

How does the ‘confidence score’ relate to the potential match result?

The system returns potential matches based on a confidence score, where the system believes it’s a match. Up to ten results are returned in reverse rank order. It is important that the user make a visual judgment, along with standard investigative
techniques and their agency's operational policies, to determine whether an actual match between the probe image and the record on file exists.

Are the field-acquired images retained in the system?

No. The algorithm creates a temporary biometric template of the field-acquired image for matching purposes and then discards it.

Once a law enforcement agency employee is approved to use the system how do they access the data?

Approved law enforcement agency employees access the ARJIS facial recognition system through a mobile Android application entitled TACIDS. This application does not work over standard cellular Internet. The mobile device must be directly attached to the ARJIS private, law enforcement network in order to access the system.

Access also requires the use of a valid ARJIS username and password, which is controlled by each agency's dedicated ARJIS Terminal Coordinators.

Does TACIDS collect information such as name, date of birth, etc. from the user?

No. The mobile application is used strictly for finding matches between probe images and mugshot images already on file.

How is the system audited?

The system logs each user's activity by agency, user-ID, date, time, and image submitted for comparison. ARJIS Information Technology personnel perform periodic sample audits to the system to ensure that it is functioning properly and that required data is being appropriately submitted by requesting agencies.

Has consideration been given to the privacy impact of facial recognition use?

The National Law Enforcement Telecommunications System (Nlets) conducted a national workshop in 2010 to address the use of facial recognition by law enforcement personnel, focusing on driver's license photo repositories across state lines. ARJIS participated in this workshop. The ARJIS facial recognition system is much more narrow, in that the photos used are derived from local booking records. The basic principles of the Nlets study and resulting publication are the same. The ARJIS privacy impact assessment can be found at https://www.arjisnet.org/.
Automated Regional Justice Information System (ARJIS)
Acceptable Use Policy for
Facial Recognition
A. STATEMENT OF PURPOSE

The purpose of this document is to outline the responsibilities of the Automated Regional Justice Information System (ARJIS) in its role as a law enforcement information technology services provider for mobile facial recognition efforts in San Diego County. ARJIS has implemented a regional facial recognition system known as Tactical Identification System (TACIDS) in support of law enforcement efforts to enhance positive identification and improve public safety.

ARJIS provides the secure network infrastructure, technical standards, security protocols, controlled access, database administration, and configuration of mobile devices for access to this system. Included in the support of the secure infrastructure are ongoing system procedures, maintenance, user access, and security monitoring of the circuits, hubs, routers, firewalls, databases, etc. These components that comprise the ARJIS Enterprise ensure the priority, integrity, and availability of services to authorized law enforcement users. This Acceptable Use Policy sets forth rules restricting how TACIDS may be accessed and defines how it is maintained by ARJIS.

The Regional Facial Recognition Operational Protocol under development by the San Diego County Chiefs’ and Sheriff’s Association outlines facial recognition best practices and standard operating procedures for those agencies that utilize facial recognition in the field.

B. FACIAL RECOGNITION OVERVIEW

Facial recognition refers to an automated process of matching facial images, utilizing algorithms and biometric scanning technologies. A biometric indicator is any human physical or biological feature that can be measured and used for the purpose of automated or semi-automated identification.

During enrollment, the facial recognition system acquires a facial image and measures distinctive characteristics including but not limited to the distance between the eyes, width of the nose, and the depth of the eye sockets. These characteristics are known as nodal points and each human face has multiple nodal points recognizable by facial recognition software.

The nodal points are extracted from the facial image and are transformed through the use of algorithms into a unique file called a template. A template is a reduced set of data that represents the unique features of the enrolled person’s face. For identification purposes, the facial recognition system compares the biometric template created from the image captured in the field with all biometric templates stored in the database. For verification purposes, the biometric template of the claimed identity will be retrieved from the database and compared with the biometric template data created from the recently captured facial image.

1. Specification of Use

There are two primary objectives of the TACIDS application. The first is assisting in the identification of individuals who have been detained based on reasonable suspicion, and are lacking and/or not forthcoming with their identification, or who appear to be using someone else’s identification or a false identification. Often times, these situations require officers to escort individuals to a police station to verify their identification. This is a time consuming process that involves taking police resources off the streets which can impact resource
availability and subsequent response time. TACIDS enhances field operations in these cases. The second objective is to assist in identifying persons who are incapacitated or otherwise unable to provide identification, including deceased or incapacitated individuals.

Officers from authorized agencies use an ARJIS enabled tablet or smartphone to access TACIDS to take a photograph of the individual. Once the photo has been submitted to TACIDS, a biometric algorithm compares the image to the local San Diego booking database (currently about 1.4 million images) and potential matches are returned within 10 to 15 seconds, in ranked order, based on the confidence level of the match.

The confidence score is mathematically calculated based on the accuracy of the biometric algorithm. If the system determines that there are potential matches, the photo captured in the field and the matching booking photos can be viewed side by side to further assist the officer in determining whether there is an actual match. Data from the booking records are displayed along with the images to assist the officer in identifying the individual.

All potential matches are considered advisory in nature and any subsequent verification of the individual's identity and/or follow-on action should be based on an agency's standard operating procedures.

2. Privacy and Data Quality

2a. Privacy

Prior to the implementation of TACIDS, in December 2010, ARJIS participated in a Privacy Impact Assessment (PIA) effort led by the International Justice and Public Safety Network, in cooperation with the United States Department of Homeland Security. This effort involved the review of existing local, state, and federal laws, and the resulting PIA contributed to the development of this Policy.

Access to and use of TACIDS data is for official law enforcement purposes only. Accessing and/or releasing data from TACIDS for non-law enforcement purposes is prohibited. TACIDS data access and use is governed by the California Department of Justice (CaDOJ) California Law Enforcement Telecommunications System (CLETs) Policies, Practices and Procedures (PPP) (current rev. 09/2014), via a Master Control Agreement (MCA) between the San Diego County Sheriff's Department (Sheriff) and ARJIS. The CLETs PPP further references the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy (current rev. 5.3, 8/4/2014).

2b. Source Data and Photo Enrollment Method

ARJIS relies on the Sheriff's booking system to provide the booking images and associated data fields that are utilized in the system for matching of field-generated photos. The booking images conform to National Institute of Standards and Technology standards. Each booking photo is enrolled by utilizing a complex mathematical algorithm to convert the photo into a set of alphanumeric characters that represent the features on the subject's face. These photos are received daily from the Sheriff through a secure automated interface. The photos are stored in a regional database, hosted, and
maintained by ARJIS. Only select ARJIS authorized technical staff has access to the booking photo database.

3. **Data Limitation**

The TACIDS system exists for the sole purpose of identifying individuals for authorized public safety purposes. The photographs taken in the field are matched only against the Sheriff's booking photo database. No other databases, such as drivers’ licenses photo databases, are linked to or accessible via TACIDS. In addition there is no interface of TACIDS to any form of video surveillance.

4. **Performance Evaluation**

In addition to audit reports, ARJIS staff regularly monitors the TACIDS system for performance, reliability, and functionality. Staff also provides system generated management reports for the participating agencies that highlight agency use, the number of matches with a 90 percent or better confidence rating, and any technical issues identified during the reporting period. Other system-generated reports are produced on an as-needed basis.

5. **Transparency and Notice**

ARJIS is a Joint Powers Agency governed by the San Diego Association of Governments (SANDAG) Public Safety Committee, which includes elected officials representing the subregions of San Diego County and public safety officials.

The acquisition of TACIDS was a competitively bid procurement. A PIA was completed and published prior to implementation of TACIDS.

This policy, the associated PIA, and other governing documents are currently posted on the ARJIS website – ARJIS.org.

6. **Security**

ARJIS is responsible for the maintenance of the TACIDS server, software upgrades, network infrastructure, and the coordination of system access.

TACIDS is hosted within the ARJIS secure infrastructure and is physically located in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections. Physical access is limited to authorized personnel that have completed background investigations and completed the relevant FBI CJIS training.

ARJIS utilizes strong multi-factor authentication, encrypted communications, firewalls, and other reasonable physical, technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system.

ARJIS meets both the CalDOJ CLETS and FBI CJIS Security Policies, which include certified FIPS 140.2 compliance (U.S. Government computer security standard), antivirus, and mobile device management software. The ARJIS mobile platform currently provides a set of statically
assigned IP address blocks to each regional agency, and working with the mobile data partners, ARJIS has established a Mobile Provider Network (MPN).

The MPN solution provides a pathway for any device that is provisioned with the ARJIS MPN configuration to directly connect and route data from the mobile device, to the carrier’s cellular tower and straight through to the ARJIS network, without interruption. ARJIS chose to use statically assigned IP addresses specifically to address any potential security concerns and to maintain the most complete control over the network and data security. This also provides ARJIS with the ability to control the flow of data traffic to the device.

Effectively, ARJIS considers any device provisioned within the ARJIS MPN solution to be a client device, and as such maintains several layers of security that allow ARJIS to stop, re-route, or terminate service to any one agency at any time, while continuing to provide service to other participating agencies. Since ARJIS is responsible for device configuration and IP assignment, ARJIS is able to immediately suspend or terminate a device without relying on mobile carriers to make changes.

7. Retention, Access, and Use Of Facial Recognition Data

7a. Retention

Data retained within TACIDS includes the following, with corresponding retention periods:

1. Initial booking records, including booking photos that are sent by the Sheriff – this data is owned and managed by the Sheriff, who sets its retention schedule

2. Internal roster of system users – continually maintained and updated as users are added/deleted

3. Activity logs – retained for a minimum of three years

4. Images on mobile devices – deleted per the law enforcement agencies’ Regional Facial Recognition Operational Protocol schedule (currently proposed at 24 hours)

7b. Requirements for All Users Accessing TACIDS

Prior to utilizing TACIDS an agency must comply with the following:

• Be an ARJIS public safety member agency

• Be a CLETS-certified agency

• Comply with applicable FBI CJIS security policies

• Designate a security officer, responsible for authorizing system access and managing user accounts
Only those authorized law enforcement personnel who have met the minimum requirements of completing CLETS certification, FBI CJIS Security Awareness Training, and background checks required for access to criminal justice data may access TACIDS. Authorization is managed by each agency's security officer.

Authorized users must have an ARJIS account and are mandated to follow the procedures for establishing complex passwords that must be changed every 90 days. TACIDS users are required to sign an agreement upon issuance of a TACIDS-enabled device certifying that they have read and will comply with this Policy. All access and use is logged and subject to audit in accordance with the procedures outlined in the audit section below.

7c. Use of TACIDS Data

TACIDS is to be used solely to assist law enforcement officers in the identification of individuals consistent with the Specification of Use set forth above.

Potential matches presented by TACIDS are considered advisory in nature and any subsequent verification of the individual's identity and/or follow-on action should be based on an agency's standard operating procedures.

8. Auditing and Accountability

TACIDS also includes preset queries to the database for auditing and other tracking functions. Capabilities include: tracking accounts, general usage, session logs, enrolled devices, and other key system components.

Access to, and use of, facial recognition data is logged for audit purposes. Audit logs shall be maintained for a minimum of three years. Audit reports are structured in a format that is understandable and useful and will contain at minimum:

- The name and ARJIS ID of the law enforcement user;
- The name of the agency employing the user;
- The date and time of access
- A copy of the biometric template created at the time of the photo capture

ARJIS will provide specific information regarding individual access and query upon request from the associated member agency. Identifying and addressing intentional misconduct is the responsibility of the individual agency. Notwithstanding the agency's responsibility with regard to misconduct, ARJIS reserves the right to enforce this Policy as described below.

9. Enforcement of Policy

Violation of this Policy by an ARJIS member agency or its staff may lead to suspension or termination of an agency or particular agency staff person's access to TACIDS. In the event a
member agency discovers suspected or actual misuse of TACIDS, it will immediately inform the Director of ARJIS, who will in turn immediately notify the SANDAG Director of Technical Services and SANDAG Executive Director. In the event ARJIS discovers suspected or actual misuse of TACIDS, the Director of ARJIS will immediately notify the SANDAG Director of Technical Services, the SANDAG Executive Director, and the member agency. The Technical Services Director, in consultation with the Director of ARJIS, or their designees, will determine whether to suspend or terminate access and if so for whom the suspension or termination will apply and will notify the affected member agency. The affected member agency will be notified of the decision by SANDAG and then will have 10 calendar days to appeal the decision to the SANDAG Executive Director. The Executive Director shall have final decision-making authority.

10. Policy Revisions

The Acceptable Use Policy for Facial Recognition will be brought to the SANDAG Public Safety Committee and the SANDAG Board of Directors at least once per year for review and determination regarding the need for amendments.

Updates regarding the TACIDS system will be provided to the SANDAG Public Safety and Chiefs'/Sheriff's Management Committees annually or upon request.

11. Indemnification

Each user of the TACIDS system (User) agrees to indemnify and hold SANDAG and ARJIS, and each of their personnel, harmless from any claim or demand, including reasonable attorneys' fees, made by any third-party in connection with or arising out of use of the TACIDS system, User's violation of any terms or conditions of this Policy, User's violation of applicable laws, regulations or other policies, or User's violation of any rights of another person or entity. The term "Users" is defined to include each agency accessing the TACIDS system, as well as each individual person with access to the TACIDS system.
I. **PURPOSE**

This Department procedure establishes guidelines for Department personnel using facial recognition field identification technology.

II. **SCOPE**

This procedure applies to all members of the Department.

III. **BACKGROUND**

San Diego regional law enforcement mobile facial recognition technology was developed for the express purpose of assisting officers in identifying persons lawfully detained or otherwise the subject of a criminal investigation, when those persons are unwilling or unable to provide proof of their identity as required by law.

IV. **DEFINITIONS**

A. **Face First –** An Android facial recognition application that operates over secure cellular wireless connectivity. A probe image is acquired then transmitted to the application, where a biometric algorithm compares the probe image with images already on file and associated with personal identifying information. The application then returns a photographic list of potential match candidates back to the officer via the Android device.
The officer reviews the list and makes a judgment, based on a visual assessment, whether the person present matches a photo within the candidate list.

B. TACIDS (Tactical Identification System) – The regional facial recognition system ARJIS, in cooperation with the San Diego Sheriff’s Department’s Jail Information Management System, maintains in support of legitimate law enforcement efforts to provide public safety.

C. Enrolled image – Sheriff’s booking photograph from TACIDS database.

V. PROCEDURES

When practical, and when it will not negatively impact officer safety, law enforcement officers should first request verification of an individual’s identity through a query of his or her name, date of birth, and other self-reported identifiers. When verification is not possible, or if the officer reasonably suspects the self-reported information is false, officers may request facial recognition field identification results.

A. Obtaining Probe Images for Comparison

The policy of the San Diego Police Department in regards to taking photographs of individuals is the same for juveniles and adults. An officer may photograph a person either in the field or at a police station under the following conditions:

1. The person is under arrest for a crime; or
2. The person is being detained as a suspect in a particular crime; or
3. The person is being legally detained for a criminal investigation.

B. Requesting Facial Recognition Comparison Information

Officers may request a facial recognition comparison from TACIDS for the following reasons:

1. To identify a suspect of a criminal investigation; or
2. To aid in locating a missing person; or
3. To identify an individual for whom a warrant has been issued.

C. Deletion of Stored Images on Device
After completing the request for facial recognition field identification results, the image used for comparison shall be manually deleted from the device used to capture the image.

VI. **RESTRICTIONS**

A. Law enforcement officers shall not request facial recognition field identification results when an individual presents a valid driver license or state identification card unless:

1. The officer reasonably suspects the driver license or identification card is forged, altered, or otherwise fraudulent; or

2. The officer reasonably suspects the individual is presenting, as his or her own, a driver license or identification card issued to another person.

B. Law enforcement officers shall only access the personal identifying information of an individual whose facial image is contained in the results of a facial recognition field identification query:

1. After determining that the individual’s enrolled image reasonably matches the probe image submitted for comparison; or

2. When the personal identifying information of the person in the enrolled comparison photo would reasonably assist the officer in verifying the identity of the person arrested or detained.

C. Dissemination of facial images and other personal identifying information obtained through the use of a facial recognition field identification tool is prohibited, subject only to the following specific exceptions:

1. Public Safety exception – When the Chief of Police reasonably determines that an individual poses a threat of substantial harm to the public, facial images and relevant personal identifying information may be released to the public.

2. Warrant exception – When a warrant has been issued for a known suspect, and the suspect’s facial image has been verified, the suspect’s facial image may be publicly disclosed for the purpose of locating the suspect or protecting the public.

3. Missing Person exception – Upon verification, the facial image of an individual reported missing may be publicly disclosed to help authorities locate the missing person.
VII. TRAINING

Department Members shall be trained in the following areas prior to utilizing facial recognition field identification:

A. The proper and legal use of facial images for facial recognition purposes;

B. How to take high quality facial images in the field for best results;

C. How to interpret the facial recognition comparison results obtained via a facial recognition field identification tool and not base decisions entirely upon the comparison results;

D. The appropriate use and sharing of information obtained from a facial recognition identification tool; and

E. The deletion of the probe image used for comparison from the device used to capture the image.

Members who have not received this training may not utilize facial recognition field identification technology.
OFFICE OF COUNCILMEMBER TODD GLORIA
CITY OF SAN DIEGO

MEMORANDUM

DATE: August 27, 2015

TO: Honorable Mayor Kevin Faulconer

FROM: Councilmember Todd Gloria

SUBJECT: Call for Development of Use Policies for Surveillance Technologies and a Citywide Privacy Policy

I am requesting your assistance to make San Diego a leader in transparency and limit the liability posed to the City by ensuring there are adequate policies regulating surveillance technology. I ask you to take steps to develop a citywide strategy on data collection, use, and retention in all departments to preserve San Diegos’ right to privacy and protect personal information.

Many City of San Diego departments collect, manage, and retain sensitive or potentially sensitive data including personnel information, attorney-client privileged communications, and credit card information, among many other data types. The potential liability arising from data breach, abuse, or misuse due to lack of training or clear use policies poses significant legal and financial risks for the City, and also puts citizens at risk.

Further, national news outlets have recently reported on San Diego’s lack of adequate policies guiding the use of surveillance technologies including international mobile subscriber identity (IMSI) catchers, license plate readers, facial recognition technology, camera equipped drones, and body cameras.

As I have stated in meetings with you and in public hearings, it concerns me that the deployment of surveillance technology including Stingray, an IMSI catcher, occurred without notice to or oversight by the Mayor’s office or the City Council. I was only made aware of the San Diego Police Department’s (SDPD) use of Stingray after a nonprofit legal advocacy organization was able to obtain purchase order documents released by the City Attorney’s office in December 2014. I have raised my concerns regarding the lack of oversight and accountability with respect to procurement of surveillance equipment this year at the April 21 and August 4 City Council meetings during grant items for the SDPD and the Office of Homeland Security (OHS). The Mayor and City Council serve a crucial role in the deployment of these programs.

To ensure transparency and limit liability, I ask that, prior to year’s end, the City undergo an effort to take an inventory of the sensitive data it collects and work with all appropriate departments and the City Attorney’s office to address vulnerabilities and develop or bolster current policies to minimize risk to the City and protect those who do business with us. I also request an informational item focusing on surveillance technology used by the SDPD and the OHS at an upcoming meeting of the Public Safety and Livable Neighborhoods Committee.
I stand behind our City employees and support them having the latest technology necessary to maximize their effectiveness in serving and protecting the people of San Diego. However, without clear guidance on how to successfully limit surveillance and data collection to individuals under warranted criminal investigation, the potential for misuse that exists may have detrimental ramifications. This could negatively impact our citizens’ civil liberties and San Diego’s commitment to Community Oriented Policing recommended by the Department of Justice in its 2015 assessment performed by the Police Executive Research Forum (PERF). The PERF report emphasized a move toward greater policy development to fill identified gaps and increase accountability and oversight.

Further, I respectfully request answers to the following questions:

1. Please provide existing standard use policies for surveillance technology the SDPD currently uses including but not limited to: Stingray/IMSI Catchers, License Plate Readers, Facial Recognition Technology, Drones, Body Worn Cameras, and Surveillance Cameras. If existing policies are not in place, please advise as to the timing for policy development.

2. What other similar technology does the City currently have?

3. How many of each of the types of technology described above does the City currently own and are there foreseeable increases to those inventories in the next five fiscal years?

4. How often and with what frequency have the technology described above been used since acquisition?

5. Does the technology described above require warrants and are there exemptions to retroactively seek out warrants when using them?

6. For each of the types of technology described above, does the existing policy limit use to an official of certain standing or require supervisor approval prior to use?

7. Does the SDPD have a way to audit use of the technology to increase accountability and decrease the potential for abuse?

8. Have the Mayor, City Council, or City Attorney had an opportunity to review any of the existing use policies that govern the use of any of the technology described above?

I look forward to your response and am available to assist in any way as we recommit to fostering the public’s trust and make San Diego a leader in transparency, accountability, and oversight.

cc: Honorable Council President Pro Tem Marti Emerald, Chair Public Safety and Livable Neighborhoods Committee
Honorable City Attorney Jan Goldsmith
Scott Chadwick, Chief Operating Officer
Hi Adrian,

I hope you are doing well. I apologize for the delay in getting this document to you as it’s been a whirlwind of transition recently. Attached is a memo that outlines some ACLU privacy concerns regarding SDPD’s facial recognition technology policies as well as some recommendations to address these concerns.

Also, I don’t know if your office has seen, but the Electronic Frontier Foundation released a number of documents it got from a PRA to SDPD (https://www.muckrock.com/foi/san-diego-56/mobile-biometric-technologies-san-diego-police-department-20388/) and SANDAG (https://www.muckrock.com/foi/san-diego-56/mobile-biometric-technologies-nagarjis-20464/). There is a good amount of information regarding the facial recognition policies that were released which I hope to go through.

Please feel free to reach out with any updates or if there is anything we can assist with.

Best regards,
Amanda

Amanda Le | Policy Associate
ACLU of San Diego and Imperial Counties
Increasing Transparency, Accountability and Oversight in adopting new Technologies
Addressing San Diego Police Department’s Facial Recognition Policies

Recommendations

San Diego Police Department’s current facial recognition policies raise significant privacy concerns. San Diego can and should take simple steps to inform the public about how this program functions by:

- Requesting that the San Diego Police Department present to the Public Safety and Livable Neighborhoods Committee on all the surveillance technologies they are currently deploying and their purported efficacy and cost.
- San Diego Police Department should amend their policies to include language that prohibits uses that violate civil liberties, the collection of other types of data such as location and retention of any and all types of electronic information.
- Lastly, it is essential that the City of San Diego adopt a Surveillance Ordinance to prevent future breaches of transparency and accountability when adopting new technologies.

Background

Under a federally funded pilot program, facial recognition technology has been in use in San Diego since 2011, but there were no policies in place surrounding this specific technology until June 2015. Since the program’s introduction of facial recognition software as a “test product for the region”, there have been more than 20,600 occasions in which the software was used by 26 local law enforcement agencies to identify individuals. As for how this technology is used in San Diego, officers in the field are equipped with Android devices featuring an application called Face First. Photographs taken by the device are called “probe images” and are sent over the cellular network to TACIDS, where it is compared against the stored templates. The officers then receive a series of enrolled photographs that matched nodal points and an estimate of how confident the software is that there was a match (these are sorted by confidence level). Officers can access the personal information of the person in the enrolled photograph through the program, but are trained to do so only if they reasonably believe that the person in the photo either is the detainee or that knowing who the person in the photo is will help them to identify the detainee.

Problem: Civil liberties and Privacy Concerns

State and local law enforcement usage of surveillance technology is fraught with privacy concerns, which are exacerbated by federal funding incentives that lead to easy access and approval for surveillance technology without public knowledge or input. While the San Diego policy for use of facial recognition

---

2 Ibid.
3 Tactical Identification System (“TACIDS”) uses booking photographs from the Sheriff’s Department as a reference for probe images. SDPD Procedure 1.50 § IV(B); ARJIS Policy § 2b.
4 ARJIS Policy § 1.
technology specifically states when the technology can be used and requires that officers be trained before using the technology, the policy must be improved to address these concerns.

**Prohibition on uses that violate civil liberties** - The policy does not include prohibitions on using facial recognition technology to assist in the enforcement of immigration laws or to curtail the First Amendment rights of citizens, including protestors.6

**Prohibition on collecting other types of data** - The policy does not state whether other non-photographic data is collected by the Face First application – such as location information – or whether it is stored or associated with records associated with individuals.

**Deletion/retention** - While the policy states that officers should delete images from their devices, it does not address whether the images are retained anywhere else.7

**Auditing of effectiveness of the program** - The policy does not specify the details of how often audits are performed or what events might trigger an audit.

**Public notice and oversight of policy changes** - There is no express mechanism requiring the public to be notified of the policy changes (though there may be one in some other document governing SDPD); and

**Enforceable consequences for misuse** - San Diego Police Department policy does not include enforceable individual disciplinary consequences for its violation (though there may be one in some other document governing SDPD)8. Actual consequences are necessary for guaranteeing that this technology is not misused.

**Solution: The Need to Increase Accountability, Transparency and Oversight**

Because the San Diego facial recognition program has been in operation for multiple years, SDPD must take steps to increase transparency by providing the public with information about how this technology has actually been used and its impact (or not) on public safety goals. To do this, San Diego Police Department should present to the Public Safety and Livable Neighborhoods Committee on all the surveillance technologies they are currently deploying.

To address how surveillance technology is currently being used in San Diego, the City of San Diego should reform its existing policies to address crucial civil liberties and privacy breaches. Recommended policy reforms should include clear language that address the above concerns.

Additionally, it is essential that the public be provided with the information on surveillance technology at the time of adoption. To ensure this, the City of San Diego should pass a Privacy Ordinance not only to foster public trust and government transparency, but ensure that any further funding for current and potential surveillance technology goes through a specific and community approved process. As described in a recent ACLU of California report, key points of this ordinance should include:

---

6 The ARJIS policy states that the database may only be used to “assist law enforcement officers in the identification of individuals” and should be considered advisory. ARJIS Policy §§ 1.7c.

7 Officers must delete probe images from their devices as soon as the results are returned. SDPD Procedure 1.50 § V(C). For the images in the TACIDS database, the Sheriff “sets its retention schedule”, seemingly without any upper limit. ARJIS Policy § 7a(1).

8 Separately, the ARJIS Policy § 9 includes non-disciplinary consequences for misuse of that database.
The creation of a clear channel in which the public is notified, informed, and kept aware throughout the decision to obtain and use surveillance technology. This can be done by ensuring informed public debate at the earliest stage of the process prior to seeking funding or otherwise moving forward with surveillance technology proposals.

Ensuring that there is a determination that the benefits outweigh costs and concerns both fiscal related and civil liberties related.

Ongoing oversight and accountability is needed through proper oversight of surveillance technology use and accountability through annual reporting, review by policymakers and enforcement mechanisms.

California localities, such as Oakland, serve as a positive example of communities and city councils working together for surveillance reform and prove that privacy protection can and should be fought for on a local level.

**Organizational Allies**

**Nationwide:**

**Center for Democracy and Technology:** Based in Washington D.C. and San Francisco, the CDT promotes internet freedom, mainly through public policy.

**Electronic Privacy Information Center (“EPIC”):** Based in Washington D.C., EPIC is a public interest research group that focuses public attention on privacy and first amendment issues regarding electronic information.

**Restore the Fourth:** With local chapters throughout the nation, Restore the Fourth works to strengthen the fourth amendment to more strongly apply in electronic privacy and surveillance matters.

**Local:**

**The World Privacy Forum:** Based in San Diego, the World Privacy Forum is a non-profit, non-partisan public interest research group that works to empower people to protect their privacy rights by providing them with the knowledge, rights and tools to do so. They perform research, analysis and consumer education in the area of privacy.

**CAIR – Council on American-Islamic Relations:** With a chapter based in San Diego, the Council on American-Islamic Relations would potentially be an ally as an organization that advocates for justice, mutual understanding and the protection of civil liberties.

**Privacy Rights Clearinghouse:** Based in San Diego, CA, the group focuses on raising awareness of privacy issues to consumers and responds to, documents and advocates for fixes to concerns brought forth by consumers.

Additional organizations could be listed depending on the specific issue.

**Contact:** Amanda Le, ACLU of San Diego and Imperial Counties
CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT

PROTECTION OF SENSITIVE INFORMATION AND DATA

<table>
<thead>
<tr>
<th>Number</th>
<th>Issue</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>90.64</td>
<td>2</td>
<td>1 of 8</td>
</tr>
</tbody>
</table>

Effective Date
May 5, 2017

1. PURPOSE

1.1. To establish a policy to ensure the confidentiality and protection of Sensitive Information against unauthorized use; to establish procedures to control access to Sensitive Information so that it is only accessible by Authorized Persons; and to establish safeguards to ensure the appropriate use of Sensitive Information by Authorized Persons.

1.2. To define responsibility and procedures for granting Authorized Persons access to Sensitive Information.

1.3. To define processes by which access to Sensitive Information is administered and to develop control points in compliance with City policy.

2. SCOPE

2.1. This policy applies to all City employees in all City departments, including independent departments as authorized by the signing authorities below; and to City volunteers, contractors, vendors, and other individuals granted access to Sensitive Information under the City's control by the nature of their support or service functions.

2.2. This policy and procedures apply to all Sensitive Information created, owned, stored, managed or under the control of the City of San Diego, regardless of the media which contains the Sensitive Information, including but not limited to paper, microfilm, microfiche or any analog or digital format.

2.3. Nothing in this Administrative Regulation supersedes any stricter requirement(s) set by other authorities (i.e., local, state, and/or federal laws, rules or regulations), such as obtaining or retaining employment in a law enforcement agency; nor does this Administrative Regulation supersede any applicable, stricter rules, regulations or policies that affect access to or use of Sensitive Information. In such cases, the department head must ensure implementation or application of any such superseding rules, regulations or policies include adequately strong internal controls over Sensitive Information.

(Supersedes Administrative Regulation 90.64, Issue 1, effective July 1, 2009)

Authorized

(Signature on File)

CHIEF OPERATING OFFICER
3. DEFINITIONS

3.1. **Appointing Authority** - An unclassified, management-level position designated by the department head or higher who has the authority to grant permission for an employee or individual to be authorized for access to Sensitive Information.

3.2. **Authorized Person** - An employee or other individual who is granted permission to access or use Sensitive Information by an Appointing Authority, as approved by the Information/Data Owner, at the type and the Level of Access to the specific information required for the performance of his or her job duties.

3.3. **Authorization Acknowledgment Form** - The City's official form used to request and authorize an individual's access to or use of Sensitive Information (see Appendix). This form will be available on the City's Intranet site (CityNet) on the 'Forms' page.

3.4. **Information/Data Owner** - The department head or designee who is the primary recipient or manager of particular Sensitive Information or who has the responsibility to oversee the collection, maintenance or management of such information or data. There will only be one defined Information/Data Owner for any particular source of data; although other departments may collect and/or access the data. An Information/Data Owner may also be an Appointing Authority, as defined in Section 3.1 above.

3.5. **Level of Access** - The amount of Sensitive Information for which access is granted for any specific category or type of Sensitive Information, such as full access to all information related to a particular category or document, or limited access to only specific pieces of information (i.e., certain fields in a database) required for the performance of valid job duties.

3.6. **Personal Identifying Information** - Shall include information listed in California Penal Code Section 530.55(b), as amended (Sept. 2006), which reads, in pertinent part:

3.6.1. **Person** - A natural Person, living or deceased, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.

3.6.2. **Personal Identifying Information** - Any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license or identification number, social security number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the Person, address or routing code, telecommunication identifying
For the purpose of this policy, **Sensitive Information** shall mean:

3.7.1. **Personal Identifying Information** (as defined above), also including debit card number of an individual **Person**, and where home/personal address and telephone number are included and work/office address and telephone number are excluded (i.e., the City Directory is not considered **Sensitive Information**); and

3.7.2. Any information that is possessed by the City of San Diego which is not subject to the California Public Records Act (refer to Administrative Regulation 95.20), and which may be used for other than the intended purpose of such information, to cause harm or otherwise jeopardize the City of San Diego or any individual, or used in violation of any local, state or federal law (for example the Health Insurance Portability and Accountability Act of 1996 (HIPAA)).

3.8. **Sensitive Information Custodian** - The **Person** who manages the physical or computer-based access to **Sensitive Information**; for example an office manager or records manager who controls access to locked file rooms/cabinets, or a computer systems administrator who manages the creation of user accounts and passwords to provide specific access to particular data. A **Sensitive Information Custodian** may also be an **Information/Data Owner**, as defined in Section 3.4. above.

3.9. **Type of Access** - Refers to Read Only, Write/Create, Edit/Modify, and Delete.

4. **POLICY**

4.1. **Sensitive Information** shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her **Appointing Authority** and approved by the **Information/Data Owner**, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.2. Contractors and vendors or other non-City employees who are authorized to access or use **Sensitive Information**, shall be required to enter into agreements stating that the individuals specified for this access and their employing Contractor/Vendor agree to be contractually bound by the terms and conditions of this policy, including personal liability, as part of their contract or agreement prior to being granted access to **Sensitive Information**.

4.3. Authorization to access or use **Sensitive Information** shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an **Authorized Person**'s job duties no longer require access to or use of **Sensitive Information**, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to **Sensitive Information** extend beyond the termination of the authorizing
contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.4. The Information/Data Owner shall specify the type and the Level of Access that should be assigned to various functional roles that require access to the Sensitive Information based on an employee's or individual's job requirements.

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.6. As a standard IT security measure, Authorized Persons shall not share their User ID and/or password with anyone else, and shall not have their User ID and/or password written down in any unsecured location (e.g., anywhere around their work location). "Generic" User IDs shall not be used for system access to Sensitive Information; each Authorized Person must use an assigned, unique User ID that is directly linked with the user's name. As a standard physical security measure, Authorized Persons shall not share their building or facility access key card or key(s) with anyone else, nor shall they allow access into secured areas by unauthorized Persons.

4.7. Violation of this policy, either by unauthorized Persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

4.8. Appointing Authorities shall review the list of their employees, contractors or other individuals who they have designated as Authorized Persons with access to Sensitive Information, at least semi-annually, to ensure continued authorization is warranted and to update (add, delete or modify) the authorization list appropriately.

4.9. Information/Data Owners shall verify and document semi-annually that the Appointing Authorities performed a thorough review of authorized users in compliance with this policy (Section 4.8.), by comparing the Appointing Authority's report with a list of individuals currently authorized to access the Sensitive Information over which the Information/Data Owner has control and authority. For internal control purposes, to maintain segregation of duties, this verification must be performed by someone other than the Appointing Authority who submitted the semi-annual review of Authorized Persons. All discrepancies shall be reported back to the impacted Appointing Authority for