

San Diego's

Privacy Policy

Development

Efforts & Lessons Learned



AUTOMATED
REGIONAL JUSTICE
INFORMATION SYSTEM



IT'S NOT LAWYERS AS USUAL

Increased public interest

Edward Snowden released documents NSA's bulk collection of communication metadata

Technology advances - LPR, facial recognition and drones

FOIA requests for databases

The ACLU and Electronic Frontier Foundation stepped up efforts to draw public attention to law enforcement data collection

Particular focus on facial recognition...



HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS ROOM

NOVEMBER 7, 2013 | BY JENNIFER LYNCH AND DAVE MAASS

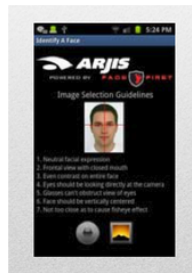


San Diego Gets in Your Face With New Mobile Identification System

The San Diego regional planning agency, **SANDAG**, has been quietly rolling out a new mobile face recognition system that will sharply change how police conduct simple stops on Americans. The system, which allows officers to use mobile devices to collect face images out in the field, already has a database of 1.4 million images and serves nearly 25 federal, state and local law enforcement agencies in the region.

Over the summer, EFF sent a California Public Records Act request to SANDAG for more information on the program. From the records we received, we've learned that the program, called "**TACIDS**" (Tactical Identification System), serves law enforcement agencies as diverse as the San Diego Sheriff's Department, the DEA, ICE, the California Highway Patrol and even the San Diego Unified School District. The officers use a **Samsung tablet or Android mobile phone** to take a picture of a person "in the field" and run that picture against databases of mugshot photos and DMV images from across several states to learn his or her identity. According to users, the system returns **high-accuracy results in about eight seconds**.

The **Center for Investigative Reporting** published an in-depth report on the program today, based in part on research conducted by EFF and the ACLU of San Diego and Imperial Counties.



HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS ROOM

JUNE 25, 2014 | BY JENNIFER LYNCH



EFF and 31 Other Organizations Call for Privacy Assessment of FBI's Biometric Database

The **FBI plans** to roll out the face recognition component of its massive Next Generation Identification (NGI) biometrics database this summer—but the Bureau has six years of catching up to do in explaining to Americans exactly how it plans to collect, use and protect this data. Today we **called** on Attorney General Eric Holder to do just that.

As we explained in the letter:

The capacity of the FBI to collect and retain information, even on innocent Americans, has grown exponentially. It is essential for the American public to have a complete picture of *all* the programs and authorities the FBI uses to track our daily lives and an understanding of how those programs affect our civil rights and civil liberties.

For this reason, it's imperative that the FBI conduct and publish a current privacy impact assessment (PIA) for NGI.

The **Privacy Act of 1974** requires all federal agencies that maintain records on Americans to explain how they collect, store, and use that information. As part of that process, agencies are **required** to perform a PIA and make that assessment available to the public. According to the DOJ's own guidelines, this is **not optional**. Despite this, DOJ has not updated its **PIA** for the face recognition component of NGI since 2008.

...and cameras on public transit

Thursday, May 7 2015 Home About Contact Search

"Investigative journalism is critical to our democracy in order to determine the truth in an objective manner."
— Bernie Kulchin, donor and board member

Categories Data Center Newsletter Become a Supporter

MTS Buses, Trolleys And Stations Tapped By An \$18 Million Surveillance Network



MTS buses, trolleys and stations tapped by an \$18 million surveillance network

Posted by: Brad Racino December 18, 2013

by **Brad Racino** | inewssource
Maps by **Joe Yerardi** | inewssource
Video by **Nic McVicker** | KPBS and Brad Racino

With millions of federal and state dollars backing them and no opposition in sight, San Diego's Metropolitan Transit System (MTS) has quietly joined the ranks of a growing number of government transportation agencies around the country that record audio — as well as video — throughout their



<http://inewssource.org/2013/12/18/mts-san-diego-surveillance/>

ACLU ACT DONATE

Adding Audio Recording to Surveillance Cameras Threatens A Whole New Level of Monitoring in American Life

By **Jay Stanley**, Senior Policy Analyst, ACLU Speech, Privacy & Technology Project
DECEMBER 20, 2012 | 11:06 AM

f t g+

There has been a lot of attention recently to the issue of audio recording being added to surveillance cameras on public buses. This issue first came onto our radar in 2009, but resurfaced again in Maryland in October (see this [October Baltimore Sun article](#)). In December the [Washington Post](#) and [The Daily](#) reported that the practice is spreading widely across the United States.



In recent decades video surveillance cameras have become commonplace in our public spaces—a trend that appears bound to increase as cameras get cheaper, smaller, and easier to connect, and as images get easier to store. The arc is long for the chilling effects of cameras but over time, if the trend continues, they will have unfortunate effects on our experience of public places.

But if we start allowing the addition of *audio* surveillance to all those cameras, that will be an enormous and significant new assault on our

SIGN UP FOR BREAKING NEWS ALERTS

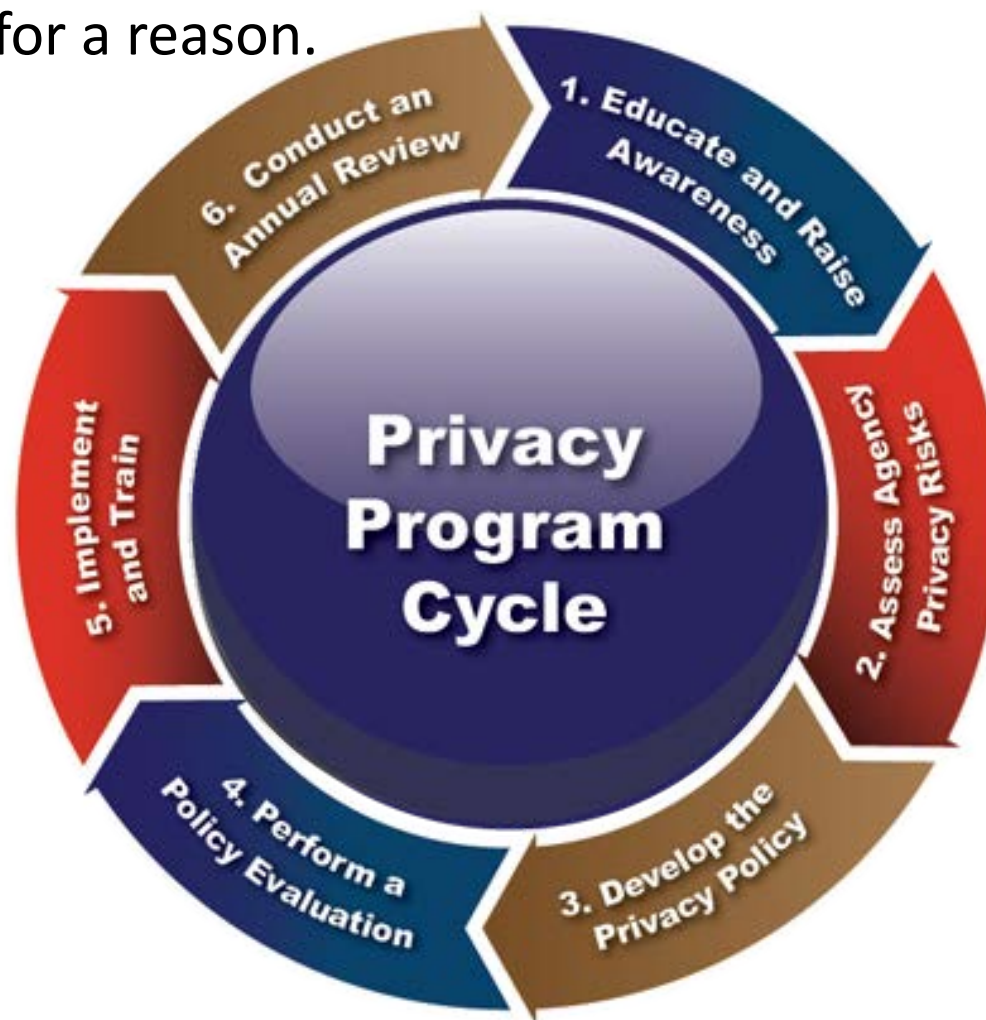
Your email address

7IP rndp

<https://www.aclu.org/blog/adding-audio-recording-surveillance-cameras-threatens-whole-new-level-monitoring-american-life>

Policy development process

Hint: It's a circle for a reason.



Stage **1** Educate and Raise Awareness

What makes a type of information “sensitive”?

Do the sensitive categories change because of technological advance?

If so, how does a type of information move into or out of the “sensitive” category?

Are facial recognition and video surveillance footage “sensitive”?

LPR example

Seattle, WA

January 23, 2013

1 patrol car's movements



Source: Bryce Newell, University of Washington Information School

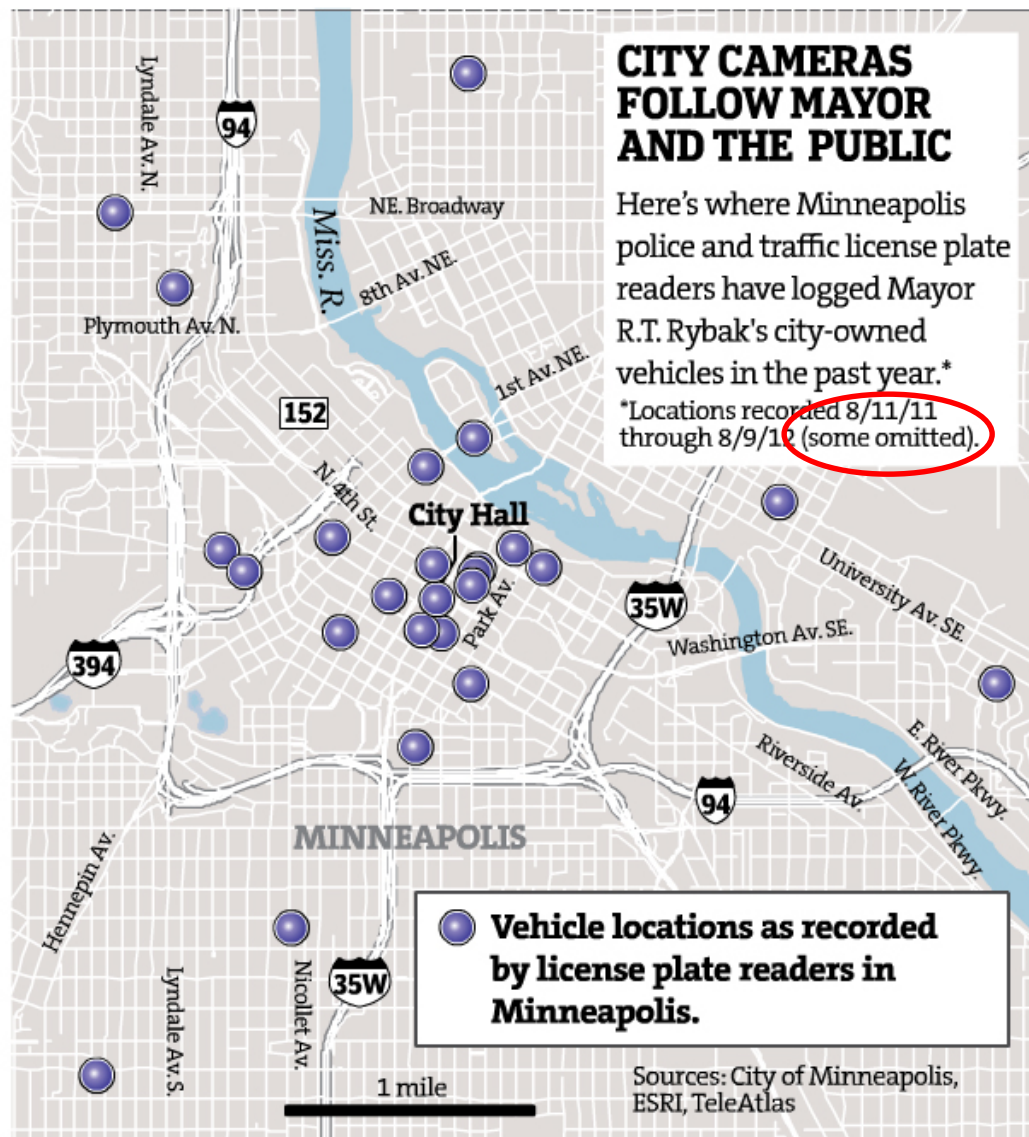
LPR Example 2

Minneapolis, MN

Aug. 11, 2011 –

Aug. 9, 2012

Locations of Mayor's city-owned vehicles



Stage **2** Assess Agency Privacy Risks

Privacy Impact Assessment

Engage stakeholders

Assess the nature of the data

Identify authorities for its collection

Articulate how data will be used

Articulate privacy risks

Construct alternative practices

ARTICULATE PRIVACY RISKS

“Brainstorming for pessimists”

Who are the actors?

Goals

Tools

Capabilities

Potential impact of misuse

How likely is each misuse?

Risk: Discriminatory surveillance

Gender

Men twice as likely to be targeted.

15% of women targeted for voyeuristic reasons

Age

65% of teenagers targeted for no reason

Race

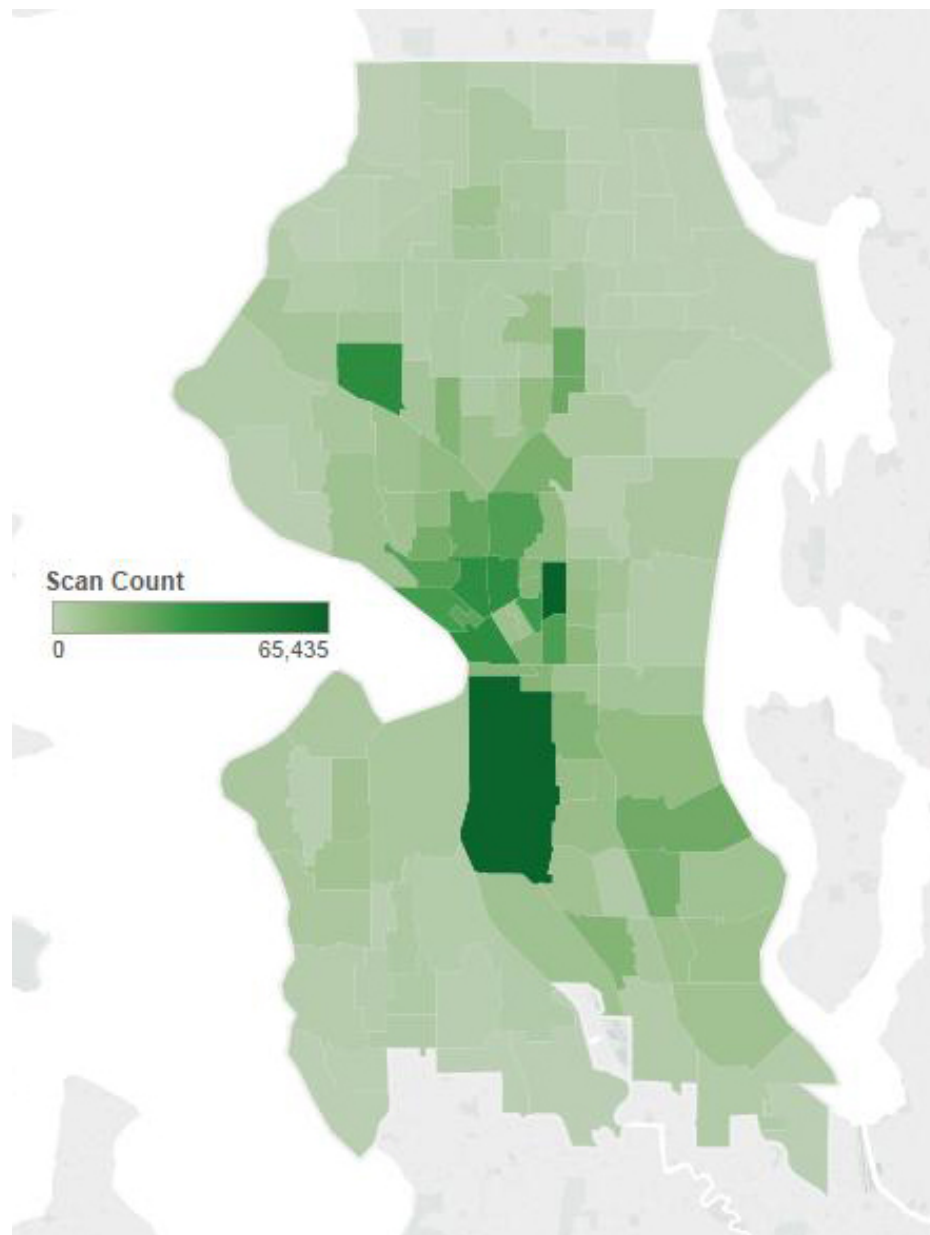
People of color were between 1.5 and 2.5 times more likely to be targeted than expected by presence in population

LPR Example

Seattle, WA

(Jan 9 - Apr 6, 2013)

ALPR Scans by Census Tract



Source: Bryce Newell, University of Washington Information School

Risk: Chilling effects of surveillance

Location information can reveal:

- Home address

- Work address

- Regular commute

- Religious affiliation

- Medical information

- Political interests

- Associations

Digital dossiers maintained by government.

Risk: Personal safety and identity theft

Geolocation data can reveal people's whereabouts.

- Outside v. Insider threats

 - Vendors with access to servers/back-ups

- Can be misused by stalkers

 - Ex spouses

 - Celebrities

 - Politicians

Remote biometrics

- Trigger same geolocation risks

- Are like SSNs - risks depends upon how it is used

CONSTRUCT ALTERNATIVE PRACTICES

Self-regulation is preferable to external regulation

Difficult to deny access based on purpose/motive

Fair Information Privacy Practices (FIPPs)

Purpose specification

Collection limitation

Use limitation

Data quality

Openness of data management practices

Individual participation

Security safeguards

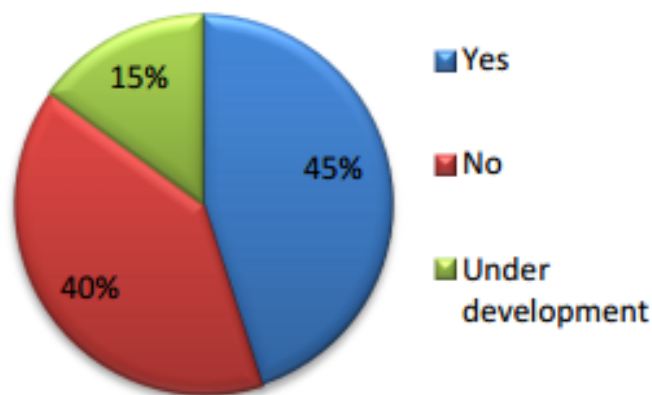
Accountability

Stage

3

Develop the Privacy Policy

7. Does your agency have any policies relating to the use of LPRs, including but not limited to, the classification or retention of LPR data? If so, please provide a copy of the policy.



MCCA Agency Use of License Plate Readers (2013).
https://www.majorcitieschiefs.com/pdf/news/mcc_lpr_survey_report.pdf

Stage 4 Perform a Policy Evaluation

Can be combined with Stage 3



<https://it.ojp.gov/gist/33/Policy-Review-Checklist>

ARJIS Mobile Facial Recognition Policy

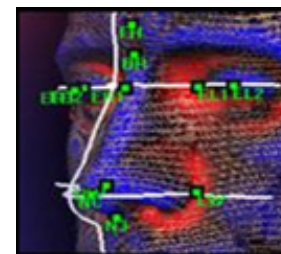
ARJIS: San Diego Public Safety IT Provider

- Provides secure network and infrastructure for 82 agencies
- Validation, and real-time uploading of public safety data
 - Maintains 47 interfaces
- Authorizes access and auditing
- Implements privacy and security protocols
- Ensures performance and reliability
- Develops technical policies
 - Align with state and national policies
- Provides region with public safety tools and technologies



ARJIS Facial Recognition Background

- National Institute of Justice (NIJ) funded grant, entitled TACIDS (Tactical Identification System) resulted in:
 - Market survey
 - Privacy Impact Assessment and Policy Guidelines
 - Proof of concept application
- Project pilot calendar year 2013
- In 2014 the US Department of Homeland Security UASI provided funding for production system
- Currently 475+ mobile devices in the field



TACIDS Functionality

- Officers use a smartphone to photograph an individual in the field when they establish criminal predicate
- Officer submits the image for comparison against the San Diego booking database (currently about 1.4 million images)
- System utilizes a mathematical algorithm for biometric comparison
- Records returned by level of confidence - highest to lowest
- Subsequent verification of the individual's identify and/or follow-on action should be based on an agency's operating procedures



TACIDS Privacy/Policy - Iterative Process

- Pilot initially leveraged Nlets PIA funded by DHS which resulted in a set of policy guidelines
- Revisions made to better address the scope of TACIDS
- Re-evaluated the policy for production system resulting in 2 documents:
 - ARJIS Acceptable Use Technical Policy for Facial Recognition – follows IACP model technology framework and FIPPS
 - Regional Facial Recognition Operational Protocol
- Approved by San Diego Chiefs and Sheriff and Board of Directors (elected officials from the 18 cities in San Diego)

Specification of Use

- o Two primary objectives for using TACIDS
 - Identification of individuals not forthcoming with their id's
 - Requires officers to escort individuals back to a police station impacts resources and response time
 - Validation of individuals using someone else's identification or a false identification
 - Fraud and identify theft on the rise
- o Potential matches are considered advisory in nature subsequent verification & follow-on action should be based on an agency's operating procedures



Privacy and Data Quality

- o Privacy Impact Assessment
- o Accessing and/or releasing data from TACIDS for non-law enforcement purposes is prohibited
- o ARJIS accesses the Sheriff's booking system to provide the booking images and associated metadata
- o Photos transmitted daily via a secure automated interface & stored in a regional database, hosted and maintained by ARJIS
- o Only select ARJIS authorized technical staff has access



Data Limitation

- TACIDS exists for the sole purpose of identifying individuals for public safety purposes. Photos 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
- No interface of TACIDS to any form of video surveillance



Transparency and Notice

- o TACIDS software was competitively bid
- o PIA was completed and published prior to implementation of TACIDS
- o Policies and related documentation are posted on the ARJIS website – www.ARJIS.org
- o May 2013 press release and news clip

ARJIS AUTOMATED REGIONAL JUSTICE INFORMATION SYSTEM

Home What is ARJIS? ARJIS Agencies Governance and Policies ARJIS Links Graffiti Tracker

ARJIS Governance

Privacy

- IACP - LPR Privacy Impact Assessment
- NLETS Facial Recognition Privacy Impact Assessment
- ARJIS Public Records Act Guidelines
- Sharing Public Transportation Agency data with Law Enforcement Agencies

Established in December of 1980, ARJIS, a Joint Powers Agency (JPA) formed under 6500 of the CA government Code, provides a criminal justice enterprise information system to the San Diego region. The ARJIS governance structure initially included the Board of Directors comprised of a primary and alternate elected official from each of the 18 Cities and the County, the Management Committee, with executive level representation from the 10 data contributing member agencies, and the Business, Technical and Crime Analysis Committees.

In 2004, ARJIS was consolidated with SANDAG and the JPA was modified to include the formation of the Public Safety Committee, replacing the ARJIS Board of Directors with representation by elected officials, law enforcement executives, emergency medical services, and homeland security officials. Governed by the Public Safety Committee (PSC) who advises the SANDAG Board of Directors, SANDAG is the only place where all of the jurisdictions (the 18 cities and the county) sit at the table and have a voice in decision making.

Policy

- FBI CJIS Security Policy
- CA DOJ CLETS Policies, Practices, and Procedures
- ARJIS Acceptable Use Policy for Facial Recognition
- ARJIS Acceptable Use Policy for Regional LPR System

Security - Physical & Electronic

- Addresses TACIDS server, software upgrades, network infrastructure and authorized system access
- Secure law enforcement facility with 24/7 security protections
- Physical access is limited to authorized personnel
- Mobile Device Management (MDM)
 - Remotely manage devices
 - Send updates
 - Immediately disable



Retention, Access and Use of Data

- Sheriff booking records owned by the Sheriff, comply with Sheriff retention schedule
- Internal roster of users
- Activity logs
- Images on mobile devices - deleted after 24 hours per the Regional Facial Recognition Operational Protocol



Retention, Access and Use of Data

- o Agency must comply with the following:
 - ARJIS public safety member agency
 - Certified CLETS agency
 - Comply with applicable FBI CJIS security policies
 - Designate a security officer
- o Authorized user
- o Follow the procedures for establishing complex passwords
- o Users sign agreement



Auditing and Accountability

- All transactions are logged
- Logs are retained for minimum of 3 years
- Audit reports are structured in understandable format
- Minimum audit information:
 - Name and ARJIS ID of the law enforcement user
 - Name of agency employing the user
 - Date and time of access
 - A copy of the biometric template created at the time of the photo capture



Stage

5

Implement and Train

- Users trained by ARJIS Mobile Program Manager
 - Sign consent form
- 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
- Suspension or termination of access may apply
- Affected member agency will be notified of the decision and have ten (10) calendar days to appeal

Stage 6 Conduct an Annual Review

Agency	Number of Queries	Potential Matches - Score 90+	Percent of Queries with Matches	Registered Users
A	5,561	1,542	28%	196
B	4,837	1,195	25%	156
C	1,536	375	24%	32
D	1,367	421	31%	46
E	1,099	256	23%	64
F	1,037	263	25%	28
G	975	228	23%	31
H	854	131	15%	33
I	838	216	26%	22
J	605	170	28%	15
K	373	68	18%	5
L	373	95	25%	25
Other	1,234	355	29%	174
Total	20,689	5,315	26%	827

Document Successes

The officer used facial recognition to id the suspect, who had assaulted a bus driver and sexually assaulted a passenger. He had absconded 18 months earlier and was a registered sex offender with two prior felony convictions for child molestation.

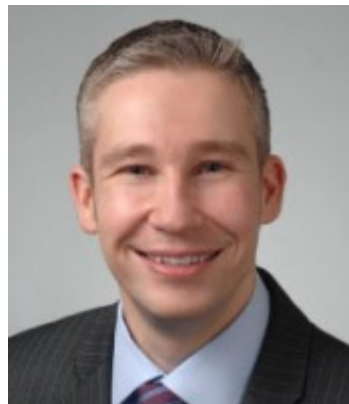
- Oceanside Police Department

Officer responded to the ER with his department issued facial recognition device in an attempt to identify a subject who was transported by medics for a possible overdose. The subject was identified with use of the device.

- National City Police Department

Questions or comments

500 N. Dearborn, 2nd Floor
Chicago, Illinois 60654
p 312.832.7891
wnagel@krasnowsaunders.com



Wil Nagel

