San Diego’s
Privacy Policy Development
Efforts & Lessons Learned
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...

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.

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

http://inewsoure.org/2013/12/18/mts-san-diego-surveillance/

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.

Image: https://it.ojp.gov/privacy
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
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
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).
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

- 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
- 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

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

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

- 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

- Authorized user
- Follow the procedures for establishing complex passwords
- 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
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
## Conduct an Annual Review

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