

1 **Tomas A. Guterres, Esq. (State Bar No. 152729)**
2 **Eric C. Brown, Esq. (State Bar No. 170410)**
3 **James C. Jardin, Esq. (State Bar No. 187482)**
4 **COLLINS COLLINS MUIR + STEWART LLP**
5 **1100 El Centro Street**
6 **South Pasadena, CA 91030**
7 **(626) 243-1100 – FAX (626) 243-1111**

*Exempt from Payment of Filing Fee
Pursuant to Govt. Code § 6103.*

8 Attorneys for Respondent
9 COUNTY OF LOS ANGELES (erroneously sued as LOS ANGELES COUNTY SHERIFF'S
10 DEPARTMENT)

11 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
12 **COUNTY OF LOS ANGELES — CENTRAL DISTRICT**

13 AMERICAN CIVIL LIBERTIES UNION) CASE NO. BS143004
14 FOUNDATION OF SOUTHERN) [Assigned to the Hon. Joanne O'Donnell, Dept. 86]
15 CALIFORNIA and ELECTRONIC)
16 FRONTIER FOUNDATION,)
17) **DECLARATION OF JOHN GAW IN**
18) **SUPPORT OF COUNTY OF LOS ANGELES'**
19) **OPPOSITION TO PETITION FOR WRIT OF**
20) **MANDAMUS**
21)
22) **DATE: March 21, 2014**
23) **TIME: 9:30 a.m.**
24) **DEPT: 86**
25) **BEFORE: Hon. Joanne O'Donnell**
26) **Petition Filed: 05/06/13**
27) **Trial Date: None**
28)

AMERICAN CIVIL LIBERTIES UNION)
FOUNDATION OF SOUTHERN)
CALIFORNIA and ELECTRONIC)
FRONTIER FOUNDATION,)
Petitioners,)
vs.)
COUNTY OF LOS ANGELES, and the LOS)
ANGELES COUNTY SHERIFF'S)
DEPARTMENT, and the CITY OF LOS)
ANGELES, and the LOS ANGELES)
POLICE DEPARTMENT,)
Respondents.)

21 I, John Gaw, declare as follows:
22 1. I am over the age of eighteen and a resident of Los Angeles County. I am employed
23 by the Los Angeles County Sheriff's Department (the "Department") as a Sergeant assigned to the
24 Technical Services Division, Communications and Fleet Management Bureau, Advanced
25 Surveillance and Protection Unit ("ASAP"), and I was thus employed by the Department at all
26 relevant times herein. I have personal knowledge of the matters set forth herein. If called as a
27 witness, I could and would competently testify as follows subject to penalty of perjury under the
28 laws of the State of California.

Collins Collins
Muir + Stewart LLP
1100 El Centro Street
So. Pasadena, CA 91030
Phone (626) 243-1100
Fax (626) 243-1111

18623

1 2. As the Sergeant of the ASAP Unit, I am responsible for the development and
2 implementation of Department policies, procedures and practices regarding the use of advanced
3 technologies, including policies, procedures and practices regarding the use of Automatic License
4 Plate Recognition technology (“ALPR technology”).

5 3. ALPR technology is a computer-based system that utilizes special cameras to
6 capture a color image as well as an infrared image of a license plate. The infrared image is
7 converted into a text file using Optical Character Recognition (“OCR”) technology. The text file is
8 automatically compared against an “informational data file” commonly referred to as a “hot list.” If
9 a match is found, the user is notified of the “hit” by an audible alert and an associated notation on
10 the user’s computer screen.

11 4. The Department uses ALPR technology to investigate specific crimes that involve
12 motor vehicles, including but not limited to stolen motor vehicles, Amber alerts that identify a
13 specific motor vehicle, warrants that relate to the owner of a specific motor vehicle, and license
14 plates of interest that relate to a specific investigation being conducted by Department investigatory
15 personnel. A recent example includes the identification and arrest of three individuals suspected of
16 the murder of Lamondre Miles on September 4, 2013.

17 5. The investigatory records that are generated by ALPR units are referred to as plate
18 scan data. Plate scan data collected from ALPR units is transmitted to an ALPR server, which
19 resides within the Department’s confidential Sheriff’s Data Network (“SDN”). Plate scan
20 information is retained for a minimum period of two years. The Department would prefer to retain
21 plate scan information indefinitely but is limited by storage considerations. In addition to the
22 software applications that are used to run the ALPR server, the ALPR server also houses the
23 “informational data file” as well as the ALPR plate scans.

24 6. Plate scan data may be queried for use in subsequent law enforcement investigations.
25 Access to plate scan data is restricted to approved law enforcement personnel within the
26 Department and within other jurisdictions that the Department shares data with. Access to plate
27 scan data is for law enforcement purposes only. Any other use of plate scan data is strictly
28 forbidden. The use of plate scan data by Department law enforcement personnel is governed by

1 Manual of Policies and Procedures sections 3-07/210.00, 3-07/220.00, and 3-07/220.20, which
2 outlines permissible uses of Department computer resources, prohibited uses of Department
3 computer resources, and penalties for violation of these policies. All Department personnel with
4 access to the SDN are required to execute a User Acknowledgment of Electronic Communications
5 Policy confirming their knowledge of and agreement to abide by Department policies and
6 procedures related to the use of the SDN.

7 7. Subject to the Manual of Policies and Procedures sections identified in Paragraph 6,
8 the Department maintains the following policies, procedures and practices regarding the use of
9 ALPR technology:

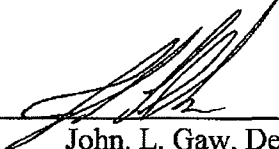
- 10 a. Century Station Order #72 – Advanced Surveillance and Protection (ASAP),
11 dated May 10, 2008. This Station Order sets forth Department policies and
12 procedures regarding the use of Advanced Surveillance and Protection
13 technologies, including ALPR technologies. A true and correct copy is attached
14 hereto as Exhibit “A.”
- 15 b. Field Operations Directive 09-04, Automated License Plate Recognition (ALPR)
16 System, dated August 17, 2009. This Field Operations Directive sets forth
17 Department policies and procedures regarding the use of ALPR technology. A
18 true and correct copy is attached hereto as Exhibit “B.”
- 19 c. Automated License Plate Recognition (ALPR) System, dated September 5, 2012.
20 This document sets forth Department policies and procedures regarding the use
21 of ALPR technology. A true and correct copy is attached hereto as Exhibit “C.”
- 22 d. Advanced Surveillance and Protection – Automatic License Plate Recognition.
23 This is a PowerPoint presentation which is used as a training aid for the use of
24 ALPR technology. The Department does not maintain user manuals for the use
25 of ALPR technology because the ALPR interfaces are intuitive and do not
26 require extensive training. A true and correct copy is attached hereto as Exhibit
27 “D.”

28 ///

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

8. Individual stations and units deploy ALPR technology subject to the policies, procedures and practices set forth in Paragraphs 6 and 7.

I declare subject to penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed this 20 day of February 2014 at Orange, California.



John. L. Gaw, Declarant

EXHIBIT "A"

CENTURY STATION ORDER #72

TITLE: ADVANCED SURVEILLANCE AND PROTECTION (ASAP)

JAMES J. HELLMOLD, CAPTAIN
May 10, 2008

PURPOSE:

The purpose of this Station Order is to outline the Policies, Procedures, and protocols for using video surveillance and advanced technologies in the field, known as Advanced Surveillance and Protection (ASAP).

POLICY:

The use of video surveillance and other advanced technologies in the field shall be guided by the United States Constitution and all applicable laws relating to a person's reasonable expectation of privacy. Specific guidelines for the practical use of ASAP technologies are guided by Department Policy, common sense, and fairness.

The Century Station Advanced Surveillance and Protection (ASAP) plan consists of the following technologies: video surveillance (recorded via automated computer server), acoustic gunshot detection with digital mapping, gunshot detection cameras, ASAP radio cars equipped with automatic license plate recognition (ALPR), fixed ALPR cameras, and other advanced technologies benefitting public and officer safety.

The primary purpose of the Century Station ASAP plan is to strengthen public safety and address quality of life issues in the community. This will be accomplished by streaming advanced technologies into the Century Station Dispatch Command Center to provide deputies with real-time intelligence in the field, and video evidence for successful prosecution when deputies are made aware of a crime. Use of video surveillance and other ASAP technologies by Department personnel shall be restricted solely for primary law enforcement functions.

Recorded information used for evidentiary purposes or requested by court order shall be booked into evidence in accordance with MPP §5-04/000. All data, including routine recordings, activity logs, and procedures regarding the CCTV system shall not be considered public information under the Public Records Act.

LOGGING PROCEDURES:

Sworn personnel may request a copy of a video recording when it relates directly to possible criminal activity. The procedures shall be as follows:

When a deputy sheriff becomes aware of video involving possible criminal activity recorded by the Century ASAP system, he/she shall notify the Watch Deputy.

The video shall be saved by the Watch Deputy or (ASAP trained personnel) under Century Station Shared Files (1-cen/sharedfiles/asap/videoevidence). Subsequently, a copy of the same video shall be burned onto a DVD for evidentiary purposes.

The video shall be saved and logged/named under the corresponding year, month, day, time of incident, and brief description of the incident. For example, the first saved video of a Lynwood shooting incident on January 5, 2008 at 1932 hours would be saved and identified in the following manner and sequence: 2008-01-05-1932-Lynwood 245

A copy of the recording shall be burned onto DVD by the Watch Deputy, clearly marked with the appropriate file number, and booked into evidence under normal protocols. The booked DVD will be considered and identified as the "original item of evidence."

If there are no ASAP trained personnel on-duty to save a copy of the video, the requesting deputy shall simply email the Century Station ASAP liaison or Detective Bureau Commander with the file name, location, date, and time of the video. The ASAP liaison will provide a copy of the recording on the next business day.

ASAP surveillance cameras are set-up to record 24 hours per day, storing the recorded video footage on a station server. The current recording capacity for Century Station ASAP server is approximately four days after which time the recorded footage is recorded over. Therefore, the watch commander shall be notified if an immediate copy of the recording is required and there are no ASAP trained personnel available to save the video.

AUTOMATIC LICENSE PLATE RECOGNITION (ALPR):

The wanted vehicle database (stolen, felony, etc.) for the ALPR system is updated 3 times per day, and may contain outdated information. Therefore whenever an ALPR camera identifies a wanted vehicle, desk personnel shall confirm the wants via MDT, CAD, or SCC prior to initialing law enforcement action. Once the vehicle's wanted status is confirmed, deputies will coordinate responding field units pursuant to established Department policy and procedures.

EXHIBIT "B"

Los Angeles County Sheriff's Department

FIELD OPERATIONS DIRECTIVE

Field Operations Support Services, (323) 526-5760



FIELD OPERATIONS DIRECTIVE: 09-04

DATE: August 17, 2009

ISSUED FOR: OFFICE OF HOMELAND SECURITY
FIELD OPERATIONS REGIONS
DETECTIVE DIVISION
TECHNICAL SERVICES DIVISION

AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM

Purpose

The purpose of this directive is to establish procedural guidelines and responsibilities of personnel and units utilizing the Automated License Plate Recognition (ALPR) system. As with any technical system, adherence to standards and procedures is a key element to the success of the system.

Background

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file" containing information on stolen or wanted vehicles as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle "hit" by an audible alert and an associated notation on the user's computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras is transmitted to an ALPR server. The ALPR server resides within the Sheriff's Data Network (SDN). In addition to software applications that are used to run the ALPR server, the ALPR server also houses the "informational data file" containing wanted, stolen, or vehicles of interest, as well as all the plate scans

Originally Issued: 08-17-09
Revised:
Latest Revision:

Page 1 of 4

Exhibit A - Page 14

captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle System (SVS), Felony Warrants System (FWS), Countywide Warrant System (CWS), and user defined "hot lists." The informational data file is updated throughout the day with different data sources being "refreshed" at different intervals. SVS/FWS data is refreshed from the state database three times per day, CWS data is refreshed from the warrant repository twice a day, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database.

When possible, confirm that the mobile ALPR unit hit information is still valid, either through the Sheriff's Communication Center (SCC) or via your Mobile Digital Terminal (MDT) prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if SCC is contacted, could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server as the scans occur. ALPR scans can be compared against the informational data file immediately when the data sources are updated.

Mobile ALPR units do not have a continuous connection to the ALPR server. In order to facilitate the exchange of data, most stations and other designated facilities have installed wireless access points which will allow connectivity to the ALPR server via wireless transmission. Once in range of a wireless access point, mobile ALPR users can activate an onboard "sync button" which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at least once at the beginning of their shift to ensure they have the latest informational data available.

Policy and Procedures

Units utilizing ALPR technology shall publish unit level policy to govern procedures on ALPR usage as well as the syncing of data between the mobile ALPR units and the ALPR server.

Mobile ALPR unit users receiving an alert that a vehicle is stolen, wanted or has a warrant associated with it shall immediately confirm the status of the vehicle by running the license plate either manually via the MDT/CAD or over the radio via SCC, unless compelling circumstances are present or officer safety issues make it unsafe to do so. In such cases, deputies shall confirm the status of the wanted vehicle as soon as possible. When requesting SCC to confirm the status of an ALPR alert, the deputy shall

advise SCC the request is for an ALPR alert on a vehicle.

In the case of a stolen vehicle alert, personnel may regard the vehicle as a known stolen vehicle, while awaiting a secondary confirmation. If the decision is made to initiate a "Code-9" due to an ALPR alert on a stolen vehicle, deputies shall advise SCC they are following a vehicle due to an ALPR stolen vehicle alert (i.e. "142F1 is code 9 on 10-29V ALPR hit") prior to receiving a secondary confirmation by MDT/SCC.

Deputies shall adhere to the Department's pursuit policy as described in the Manual of Policy and Procedures § 5-09/210.00. SCC shall immediately provide secondary confirmation or advise the unit that the vehicle is not reported as stolen.

When Desk Personnel receive an alert from a fixed ALPR system, which is the result of an image taken from a fixed camera, they shall confirm the current status of the vehicle via their CAD terminal or via SCC. While waiting for confirmation, desk personnel will advise field patrol units of the ALPR alert, the location, the vehicle description, request aero bureau, and coordinate responding field units.

Any incident associated with the ALPR system shall be documented using a secondary ALPR statistical code. The statistical code shall go on the classification line of the Incident Report (SH-R-49) and in the MDT clearance. Additionally, any vehicle recovered using the ALPR system shall have "ALPR RECOVERY" written across the top of the CHP-180 and the secondary ALPR statistical clearance code will be entered into the MDT clearance log. ALPR statistical codes cannot be used for the issuance of an URN number, but shall be used as a secondary statistical clearance code.

Please ensure the following stat codes are used:

835 - ASAP - ALPR/MOBILE
836 - ASAP - ALPR/FIXED CAMERA

Examples:

Personnel making an arrest due to an ALPR alert shall enter "835" or "836" as a secondary statistical clearance code in their MDT Log Clearance and on the Classification line of the SH-R-49 report form.

Personnel recovering a stolen vehicle with no suspect in custody shall write "ALPR-CAR RECOVERY" on the top of the CHP-180 as well as use the stat "835" as a secondary MDT Log Clearance.

Plate scan information is retained for a period of two years and may be queried for use in law enforcement investigations. Access to plate scan information is restricted to approved personnel with assigned passwords. Access to this data is for law

enforcement purposes only. Any other use of this data is strictly forbidden. Employees found using this data for anything other than law enforcement purposes will be subject to discipline under Manual of Policy and Procedures sections 3-07/210.00 Permissible Use and 3-07/220.00 Prohibitions.

Hot lists are comprised of user defined data that is manually input into the informational data file so that ALPR users will be alerted whenever a "vehicle of interest" is located. Current use of hot lists include AMBER alerts and vehicles associated with 290 sex registrants. Hot lists can be loaded into a specific station area vehicle or to ALPR all vehicles countywide.

Hot lists can be input into the ALPR server informational data file only by ALPR administrators. Unit commanders, or their designees, must approve hot list information that is intended for use solely in their area cars. With the exception of AMBER alert information entered by SCC personnel, hot list information intended for Department-wide use must have the approval of the Director of the Law Enforcement Information Sharing Program. Mobile ALPR users can input individual license plates into their patrol vehicle's ALPR system for use during their shift, however, the information will be deleted from that mobile ALPR unit once the vehicle syncs with the ALPR server. An ALPR vehicle alert identified via hot list information does not automatically provide ALPR users with sufficient justification to pullover or detain vehicle occupants. Often times, these hotlists will identify a "vehicle of interest" which is not necessarily wanted for a crime (ex: sex registrants vehicle). Personnel must use discretion and in some cases have independent information justifying a traffic stop.

Questions regarding the use of ALPR equipment or accessing plate scan information may be directed to the Advanced Surveillance and Protection Unit at

Questions regarding the content of this Field Operations Directive may be directed to Field Operations Support Services at

Affected Directives/Publication

Manual of Policy and Procedures §5-09/210.00 Pursuits

Cites/References

<http://www.pipstechnology.com/>

DRB:WJM:TPA:CWR:NBT:WJM:JLS:EPF:ef

EXHIBIT "C"

September 5, 2012

AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM

ALPR is a computer-based system that utilizes special cameras to capture a color image, as well as an infrared image, of the license plate of a passing vehicle. The infrared image is converted into a text file utilizing Optical Character Recognition (OCR) technology. The text file is automatically compared against an "informational data file" containing information on stolen or wanted vehicles, as well as vehicles associated with AMBER alerts, warrant subjects or other criteria. If a match is found, the user is notified of the vehicle "hit" by an audible alert and an associated notation on the user's computer screen.

ALPR cameras can be mobile (mounted on vehicles) or on fixed positions such as freeway overpasses or traffic signals. ALPR systems mounted on vehicles have all the necessary equipment to scan plates, notify the user of a vehicle hit, and store the plate scan data for uploading into the ALPR server at a later time. ALPR fixed positions transmit plate scan data to the ALPR server as they are scanned and notify a central dispatch, such as a station desk, of any vehicle hit.

ALPR cameras can photograph thousands of plates in a shift. All plate scan data collected from the ALPR cameras is transmitted to an ALPR server. The ALPR server resides within the Sheriff's Data Network (SDN). In addition to software applications that are used to run the ALPR server, the ALPR server also houses the "informational data file" containing wanted, stolen, or vehicles of interest, as well as all the plate scans captured by the ALPR cameras.

The informational data file is comprised of information from the Stolen Vehicle System (SVS), Felony Warrants System (FWS), Countywide Warrant System (CWS), and user defined "hot lists". The Informational data file is updated throughout the day with different data sources being "refreshed" at different intervals. SVS/FWS data is refreshed from the state database six times per day, CWS data is refreshed from the warrant repository twice a day, and hot list data is refreshed upon input into the ALPR server. It is important that ALPR users take into account the amount of lag time between receiving an ALPR hit notification and the last updating of the informational data file within the mobile ALPR unit database.

When possible, confirm that the mobile ALPR unit hit information is still valid, either through the Sheriff's Communication Center (SCC) or via your Mobile Digital Terminal (MDT) or Mobile Digital Computer (MDC), prior to taking police action. Confirmation can be deferred in rare circumstances (i.e. special investigative units) when compelling circumstances may exist that, if SCC is contacted, could jeopardize the investigation and/or officer safety.

Fixed ALPR cameras have a continuous connection to the ALPR server. They are capable of uploading plate scan data to the ALPR server within seconds of the scans occurring. ALPR scans can be compared against the informational data file immediately when the data sources are updated.

Most mobile ALPR units do not have a "continuous" connection to the ALPR server. In order to facilitate the exchange of data, most stations and other designated facilities have installed wireless access points which will allow connectivity to the ALPR server via wireless transmission. Once in range of a wireless access point, mobile ALPR users can activate an onboard "sync button" which will upload plate scan information from the vehicle to the ALPR server and/or download the latest informational data file from the ALPR server to the vehicle. It is imperative that mobile ALPR users sync their mobile units at the beginning and end of their shift to ensure they have the latest informational data available. If the ALPR system is integrated with an MDC, it is possible for the user to update their data via the unit's cellular connection in the field.

BOSS (Back Office System Server)

The BOSS server is where all the stored ALPR data resides. Within the server are the "hotlists," which are deployed and used to compare the license plates that are scanned by the ALPR cameras. The "hotlists" are maintained by the ASAP (Advanced Surveillance and Protection) Unit and are set-up to refresh automatically. There are a few cases which specific hotlists have been set-up for certain units and they have to be updated manually (most of these lists are covert hotlists and the user is not notified of the "hit"). The primary use of the server is for storage of the license plate data captured. Currently, we maintain approx. (2) years' worth of license plate data from all of our LASD ALPR cameras. Detectives and other investigative resources can utilize the BOSS database in searches for full or partial license plate information. Additionally, we have set-up links to query other LA County police agencies approx. 26 at this time, and are in the process of setting up and expanded ability to search other county law enforcement agencies with ALPR such as San Bernardino County Sheriff and Riverside County Sheriff.

Department Policies and Guidelines

There are no written guidelines as to how to use the data. The policy of how we use Department resources (data) is listed below. Keep in mind data is often used as a "lead" to glean further information on an active investigation that law enforcement handles.

Access to plate scan information is restricted to approved personnel with assigned passwords. Access to this data is for law enforcement purposes only. Any other use of this data is strictly forbidden. Employees found using this data for anything other than law enforcement purposes will be subject to discipline under Manual of Policy and Procedures sections 3-07/210.00 Permissible Use and 3-07/220.00 Prohibitions.

3-07/200.00 SHERIFF'S DATA NETWORK (SDN)

The Sheriff's Data Network (SDN) central hub is at the Sheriff's Headquarters Building and is under the administration of Data Systems Bureau.

The Sheriff's Data Network is a high speed network connecting all Sheriff's Department facilities and participating Los Angeles County municipal police departments. The SDN provides connectivity between desktop computers throughout the Department, as well as connection to other networks such as the Internet, LA Net, CLETS, and the Statewide Integrated Narcotics System. The SDN currently provides access to a wide range of applications, such as AJIS, LARCIS, CWS, CCHRS, RAPS, FMS, Cal Gangs (Formerly GREAT), CWTAPPS, JDIC and the Department's Intranet Server. For an up-to-date list of applications available on the Sheriff's Data Network, contact the Data Systems Bureau Help Desk.

3-07/210.00 PERMISSIBLE USE

The use of any Department computer resource is restricted to those activities related to Department business. Use of computers and electronic communications by employees is authorized in support of the law enforcement mission of the Department and the administrative functions that support that mission. Sheriff's Department employees and other authorized users shall adhere to this policy as well as the guidelines set forth in the County Electronic Data Communications and Internet Policies.

Employees are expected to abide by the standards of conduct delineated in other volumes, chapters and sections of the Department's Manual of Policy and Procedures as they may be applied to the use of electronic communications and use and release of information.

3-07/220.00 PROHIBITIONS

Employees shall not add, alter, copy, damage, delete, move, modify, tamper with or otherwise use or affect any data or software, computer, computer system, or computer network in order to either:

- Devise or execute any scheme or artifice to defraud, deceive, destroy or extort,
- Wrongfully control or obtain money, property, or data,
- Disrupt or cause the disruption of computer or network services, or deny or cause the denial of computer or network services to an authorized user of a Department computer, computer system, or computer network,
- Assist in providing access to unauthorized persons to any data, software, programs, computer system, or computer network.

Unless specifically authorized by Data Systems Bureau, Department employees shall not install, connect to, move, change, modify, disconnect, or tamper with any data circuit, router, switch, hub, data jack, data cable, server, or other data communications equipment or software or assist any unauthorized person in gaining access to data circuits, routers, switches, hubs, data jacks, data cables, servers, or other data communications equipment or software:

Employees shall not do any of the following without the required authorization:

- Access or allow access to another to obtain, alter, or prevent access to stored electronic communications,
- Use electronic communications to capture or open electronic communications of another, or access files without permission of the owner,
- Damage hardware, software, or other communications equipment or interfere with functionality,
- Attempt to breach any security measures on any electronic communications system, or attempt to intercept any electronic communication transmission,
- Modify or delete any file, folder or system audit, security, or ownership records or time stamp with the intent to misrepresent true system audit records,
- Access the files belonging to another for non-business purposes,
- Use someone else's USERID, password or access another person's files, or retrieve stored communications without authorization,
- Modify the hardware or software configuration on any computer,
- Use electronic communications to transmit (upload) or receive (download):
 - Any communication violating any applicable laws, regulations, or policies,
 - Proprietary or confidential Department information,
 - Chain letters,
 - Material that would be offensive to a reasonable person.
- Transmit any electronic message in violation of file size restrictions,
- Use Department computer equipment or network to send or receive electronic communications for non-Department business,
- Use computers, networks, or electronic communications to infringe on the copyright or other intellectual property rights of the County or third parties,

- Send or receive commercial software in violation of its license agreement,
- Copy personal files, programs, or images into any Department computer without authorization from their unit commander,
- Send anonymous messages or represent themselves as someone else, real or fictional, or send messages or images which are defamatory, fraudulent, threatening, harassing, sexual or contain derogatory racial or religious content,
- Establish any hidden or misidentified links on any web page,
- Send or forward messages which have been altered in order to deceive the receiver as to the original content,
- Use Department computers, networks, software, or electronic communications for personal financial, commercial, political, or other personal use,
- Use electronic communications to intimidate, embarrass, cause distress, or otherwise force unwanted attention upon others or to interfere with the ability of others to conduct Department business or create a hostile work environment,
- Use electronic communications in competition with commercial services to individuals or organizations outside the Department,
- Use electronic communications for the purposes of gambling, including but not limited to, lotteries, sports pools, and other personal wagering,
- Give out employee personal information such as home address and/or telephone numbers.

3-07/220.20 CALIFORNIA DEPARTMENT OF JUSTICE ADMONISHMENT

- As an employee of the Los Angeles County Sheriff's Department, you may have access to confidential criminal record and/or Department of Motor Vehicles record information which is controlled by statute. Misuse of such information may adversely affect the individual's civil rights and violates the law. Penal Code Section 502 prescribes the penalties relating to computer crimes. Penal Code Sections 11105 and 13300 identify who has access to criminal history information and under what circumstances it may be released. Penal Code Sections 11140 - 11144 and 13301 - 13305 prescribe penalties for misuse of criminal history information. Government Code Section 6200 prescribes the felony penalties for misuse of public records and CLETS information. Penal Code Sections 11142 and 13303 state:
- "Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person not authorized by law to receive the record or information is guilty of a misdemeanor."
- California Vehicle Code Section 1808.45 prescribes the penalties relating to misuse of Department of Motor Vehicles record information.

Any employee who is responsible for such misuse is subject to disciplinary action. Violations of this law may also result in criminal and/or civil actions.

3-07/250.00 LASD USER AUTHORIZATION AND ACKNOWLEDGMENT OF POLICIES AND GUIDELINES

Employees will be responsible for reading and signing the Sheriff's Department "User Acknowledgment of Electronic Communications Policy" form before obtaining authorization to access the Sheriff's Data Network. The Department form requires a counter signature by the user's supervisor at the rank of sergeant or higher. An employee may request authorization to access the Sheriff's Data Network by submitting the request as described under the manual section entitled, Data Communications Management (section 3-07/230.00), and attaching the signed user acknowledgment form.

User Acknowledgment of Electronic Communications Policy

I understand that the Los Angeles County Sheriff's Department requires each user, who has access to automated data communications, be responsible for adhering to its electronic communications policy sections as set forth in the Manual of Policy and Procedures, section 3-07/200.10 through section 3-07/250.00 inclusive. I have received a copy of these sections of the Manual of Policy and Procedures.

I understand that I must not have an expectation of privacy when using County electronic communications and acknowledge that my electronic communications may be monitored at any time by authorized employees.

By signing this form, I agree to abide by all policies, including state statutes relating to electronic communications and use of information, and understand that I will be held accountable for my actions, and that disciplinary actions may result from not abiding by these policies. I also agree to give authorized persons, including supervisors, auditors, and investigators access to my equipment, software, and files at reasonable times for the purposes of investigating compliance.

User Name (PRINT)
Date

User Signature

As a supervisor, by my signature, I acknowledge my responsibility to have provided the electronic communications policies, section 3-07/200.10 through section 3-07/250.00 inclusive, to the above user. I also acknowledge that I am responsible for ensuring that the above user, whom I supervise, has read and understands' this policy.

Supervisor's Name (PRINT)
Date

Supervisor's Signature

*** Attached is our Field Operations Directive as to how we utilize ALPR in the field ***

We do not have user manuals for members of the Department. We train personnel in groups utilizing the train the trainer methodology. Both interfaces of the ALPR system are intuitive and do not require extensive training.

Retention is currently limited by the size of the data stored. As we expand the number of ALPR units, we additionally have to minimize the retention of the data we keep. Currently, we would prefer to retain data indefinitely but this will change if we cannot keep up with the increasing data storage requirements. There is no national or state mandate specifically for ALPR data retention (in California) and we have looked at similar standards, such as video, which is currently (2) years.

Sergeant John Gaw
LASD / Technical Services Division
Communications and Fleet Management Bureau (CFMB)
Advanced Surveillance and Protection Unit (ASAP)
12440 East Imperial Highway, #130
Norwalk, CA 90650
(562) 345-4476 / Office
jlgaw@lasd.org
asap@lasd.org
<http://intranet.lasd.sheriff.sdn/intranet/announcements/ASAP/ASAP.shtml>
www.comptonasap.com
<http://www.lasd.org/sites/ASAP/index.html>
<http://www.youtube.com/user/LACountySheriff>



EXHIBIT "D"

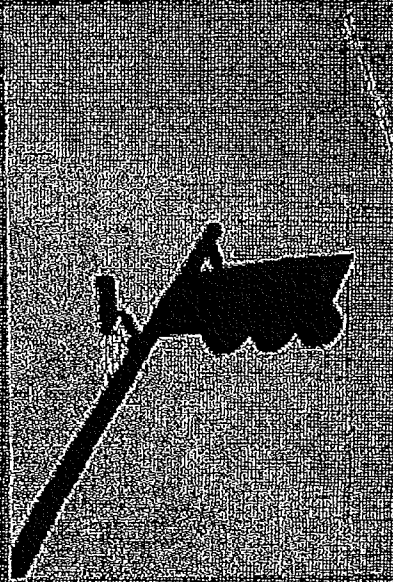
ASAP
ADVANCED SURVEILLANCE AND PROTECTION



Los Angeles County Sheriff's Department

Automatic License Plate Recognition-ALPR

Deployed on radio cars



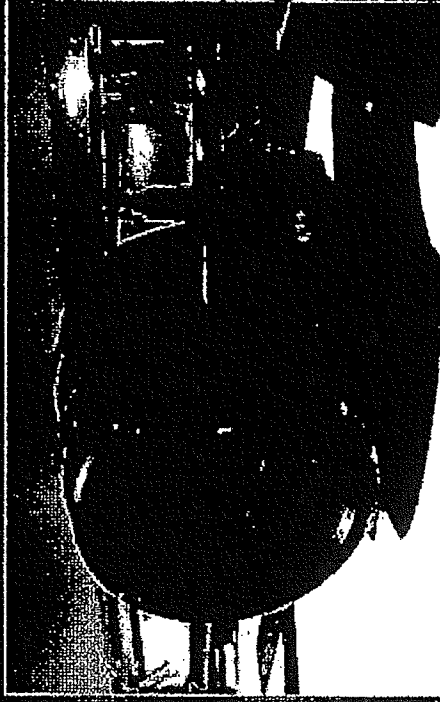
or at fixed locations

Automatic License Plate Recognition Cameras

3 camera assemblies located on
radio light bar



Each camera assembly contains a
color camera and an infrared
camera

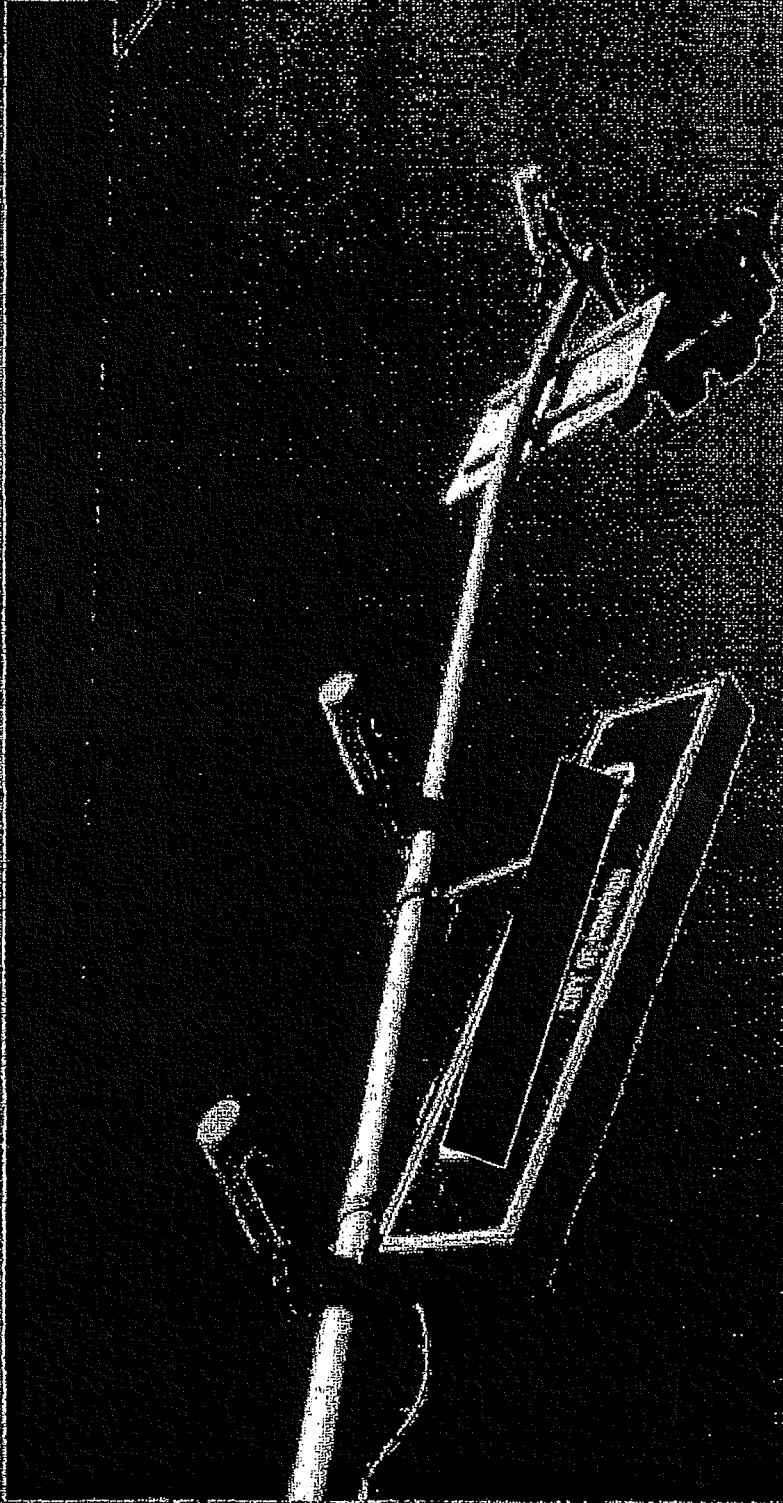


Mobile ALPR

Deputies view of monitor



Fixed Cameras in Compton






The original concept of License Plate Recognition was to identify stolen vehicles. Since it's deployment, additional applications have been implemented and continue to develop.

Benefits of ALPR/BOSS

- ALPR has the "ability" to read more than 14,000 license plates during the course of a shift (does not read black or blue);
- can read a license plate, coming in the opposite direction, at over 160mph (closing speed)
- provides an overview photograph of the vehicle and its license plate,
- imbeds a "stamp" of the date, time, GPS coordinates, and other data,
- can also obtain the license plate in difficult conditions. For example, poor lighting conditions, or when the vehicle is approaching and it's headlights make it difficult to read.

Here's an example;



PIPES
TECHNOLOGY

BOSS 47N P3A


LOGIN ID: MDR

CONFIDENCE: 98


TIME STAMP: 7/23/2009 11:41:02 AM

LOCATION: MDR-M-SD7012

GPS: 38°07'11.2" N 118°38'09.7" W



CAI: 920090714



Home

Arizona

Arizona

County

Group

Users

Locations

Yard/Off

Operations

System

PIPE

Assets

MANAGEMENT

Print

Logout

Stolen Vehicle

MAP

SATELLITE

HYBRID

PIPES

BOSS

47N P3A

Applications for ALPR

- locate wanted/stolen vehicles,
- identify vehicles with L.A. County misdemeanor warrants of \$26,000 or greater, all felony warrants, and no bail warrants,
- locate vehicles identified by the Amber alert system,
- locate vehicles which are frequently sold or not registered,
- assist in traffic enforcement by identifying drivers with outstanding DUI's, suspended license warrants, which frequently result in higher hit and runs collisions,
- monitor "party calls" where assaults and homicides sometimes occur, providing critical investigative information,
- monitor locations of suspected narcotic or gang activity,
- monitor motels where criminals may attempt to hide and evade law enforcement, or large parking lots,

- provide data for department investigators to search areas impacted by rising crime rate such as residential burglaries, vehicle burglaries and thefts.

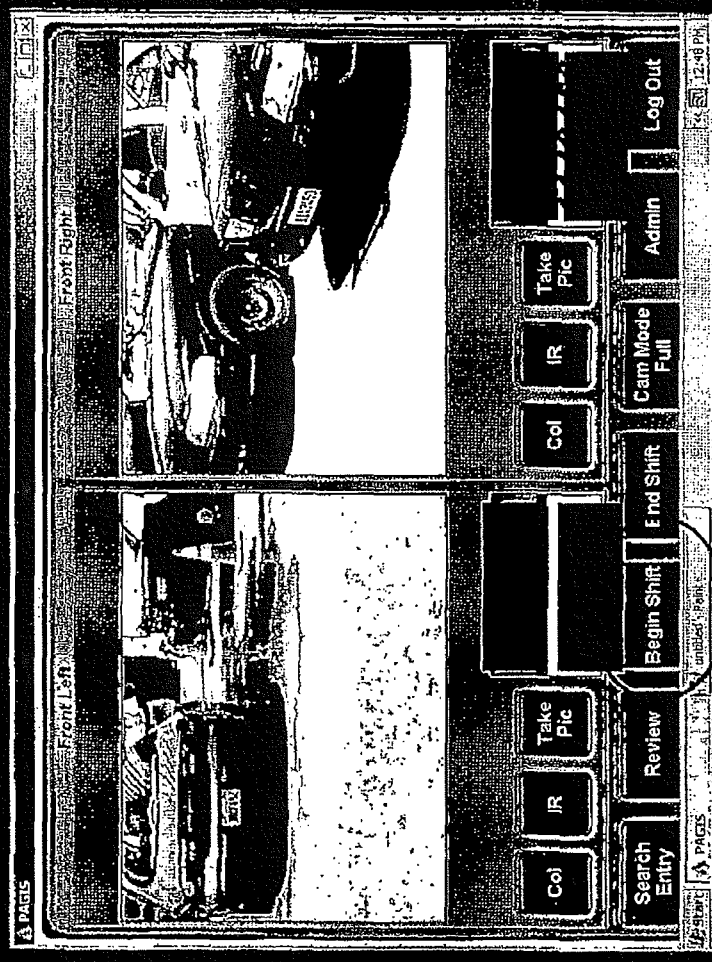
- provide data where station desk personnel can access license plate information related to "just occurred" calls. That information can be provided to responding units where detailed vehicle information can be updated from photographs in the BOSS system, extremely useful to Sheriff department. Also units, possible direction of travel or destinations can be provided, follow vehicles may be identified,

- additional victims and witnesses may be identified. Investigators have deployed ALPR in locations where a crime has occurred, identified motorists who commute in that area during that time period,

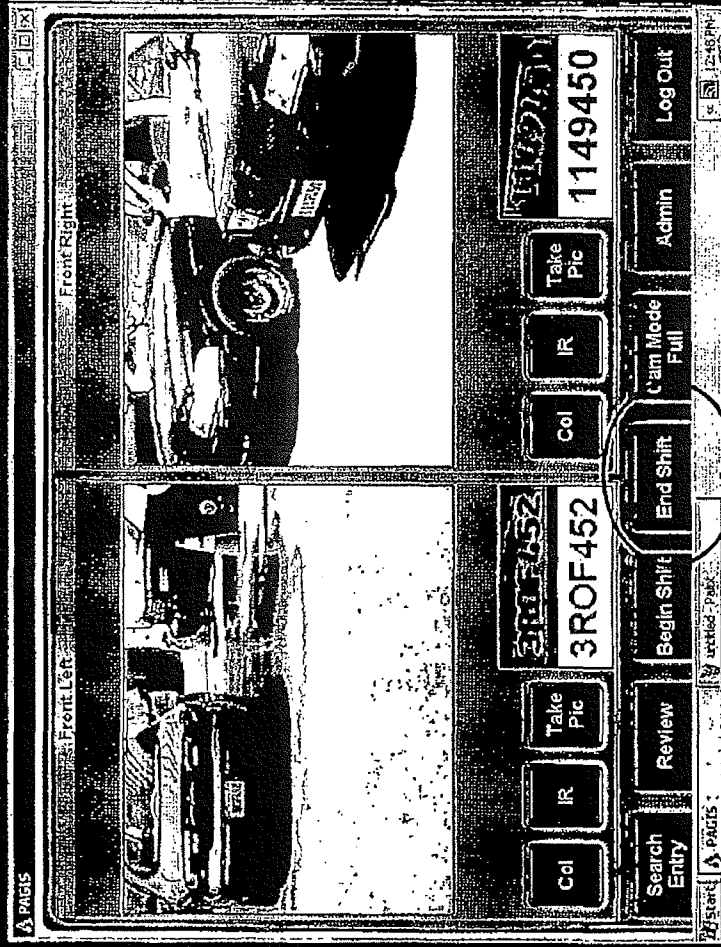
- It may also be useful in clearing someone of an allegation and help determine the truthfulness of a suspect or witness.

Brief overview of an ALPR car

Deputies will download the updated wanted/stolen information via a wireless connection at their station,



During or at the end of their shift, they can upload their scans/reads to the BOSS server which will now be available to department investigators.



Important considerations regarding access to the data:

The Department of Justice (DOJ) provides updated lists of stolen/wanted vehicles 3 times a day,

2:45 AM

10:45 AM

6:45 PM

Warrant information is updated 2 times a day,

Scans or reads are stored in the processor located in the trunk, until the deputy uploads the data at the station to the server,

Patrol deputies have the ability to manually enter license plates into their ALPR system, (i.e a 215 P.C. just occurred),

How to access the BOSS system





Internet Policy - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Print Refresh

Address <https://intranet/frz/intranet/How/DSB/InternetUsePolicy.htm> Go | Title

Google Search Bookmarks Check AutoFill



CLICK HERE FOR DETAILED INFORMATION ON:
DATA SECURITY POLICIES

INTRODUCTION:
As the Sheriff Department expands its technology offerings and makes Internet access available to all users, it is important to keep Department guidelines in mind when it comes to using computers and the Internet. For this reason your Internet Explorer default has been set to this Web Page listing the Internet Use Guidelines.

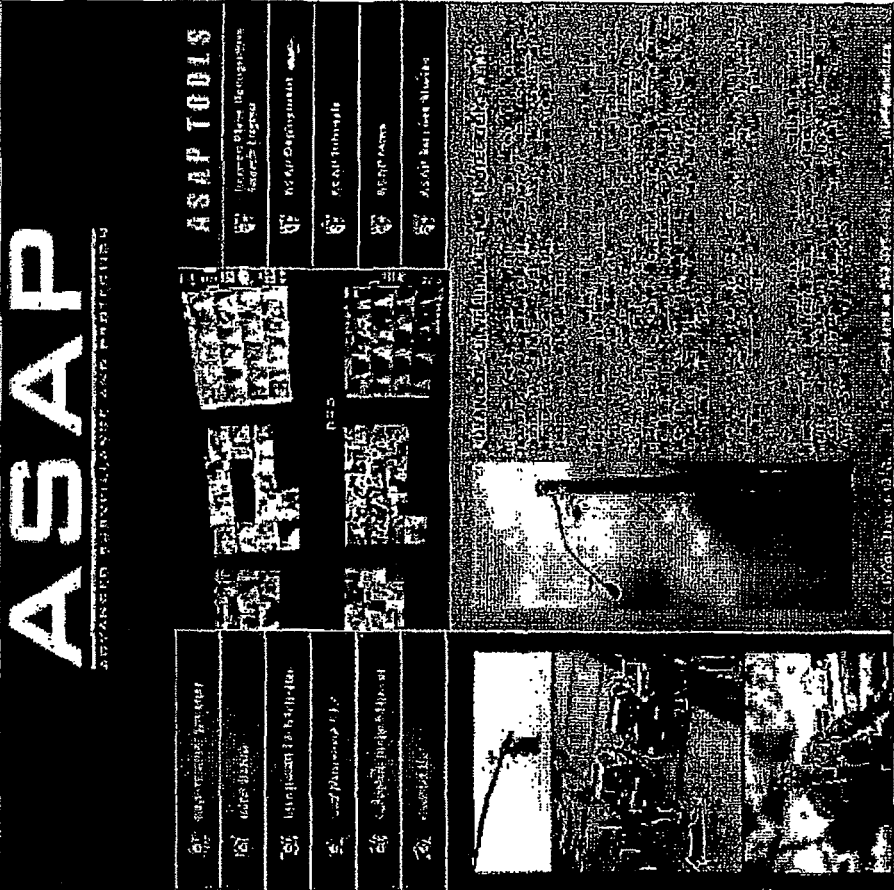
MPP 3-07/210.00 PERMISSIBLE USE:
The use of any Department computer resource is restricted to those activities related to Department business. Use of computers and electronic communications by employees is authorized in support of the law enforcement mission of the Department and the administrative functions that support that mission. Sheriff's Department employees and other authorized users must adhere to this policy as well as the guidelines set forth in the County Electronic Data Communications and Internet Policies.

*Employees are expected to abide by the standards of conduct delineated in other volumes, chapters and sections of the Department's Manual of Policy and Procedures as they may be applied to the use of electronic communications and use and release of information.

GUIDELINES:
Managing each user's Internet access will be the responsibility of the unit where the user is assigned.
A Unit Commander at his/her discretion may allow, restrict or remove Internet access for any user in their unit.
LASD will filter access to Internet sites and Internet usage in general. Web sites, Web services, or materials deemed inappropriate by the Department will be blocked and not made available to users.
All uses of LASD's Internet access service which are in violation of any federal, state or local law, County of Los Angeles Code, LASD's Policy and Procedures Manual, or these guidelines are strictly prohibited.
All Internet access through the Sheriff's Data Network is monitored and logged on an ongoing basis. LASD has the right and capability to monitor Internet usage by each user on the system.

Start

Taskbar: Microsoft Outlook BOSS - Back Office S... set PowerPoint BOSS Microsoft Plus - [SRG CAD] Internet Policy - Mic... Search with Google Local Internet 4:28 PM



ASAP is the national leader in providing...
 ASAP...
 ASAP...
 ASAP...
 ASAP...

ASAP TOOLS

- ASAP TOOLS - ASAP TOOLS
- ASAP TOOLS - ASAP TOOLS
- ASAP TOOLS - ASAP TOOLS
- ASAP TOOLS - ASAP TOOLS
- ASAP TOOLS - ASAP TOOLS

ASAP TOOLS



License Plate Recognition
Search Engine



ASAP Deployment



ASAP Tutorials



ASAP News



ASAP Success Stories

Log in screen



BOSS 47N R3A

HOME
REPORTS
ADMIN
SYSTEM
PIPS
AVAGATA
MAZ PROHIBIT
PLM
Exam Out

BOSS: Back Office System Server Copyright (C) 2007 by PIPS Technology, Inc.

LOGIN NAME:	<input type="text"/>
PASSWORD:	<input type="password"/>
<input type="button" value="Logon"/>	FORGOT YOUR LOGIN NAME OR PASSWORD?

HOME

REPORTS

ADMIN

SYSTEM

PIPS

ALARMS

MY PROFILE



PRINT

SIGN OUT

Apips EX-BOSS 47N R34

Host	IP	Port	State	Time	...
192.168.1.1	192.168.1.1	80	Open	0.000	...
192.168.1.2	192.168.1.2	80	Open	0.000	...
192.168.1.3	192.168.1.3	80	Open	0.000	...
192.168.1.4	192.168.1.4	80	Open	0.000	...
192.168.1.5	192.168.1.5	80	Open	0.000	...
192.168.1.6	192.168.1.6	80	Open	0.000	...
192.168.1.7	192.168.1.7	80	Open	0.000	...
192.168.1.8	192.168.1.8	80	Open	0.000	...
192.168.1.9	192.168.1.9	80	Open	0.000	...
192.168.1.10	192.168.1.10	80	Open	0.000	...
192.168.1.11	192.168.1.11	80	Open	0.000	...
192.168.1.12	192.168.1.12	80	Open	0.000	...
192.168.1.13	192.168.1.13	80	Open	0.000	...
192.168.1.14	192.168.1.14	80	Open	0.000	...
192.168.1.15	192.168.1.15	80	Open	0.000	...
192.168.1.16	192.168.1.16	80	Open	0.000	...
192.168.1.17	192.168.1.17	80	Open	0.000	...
192.168.1.18	192.168.1.18	80	Open	0.000	...
192.168.1.19	192.168.1.19	80	Open	0.000	...
192.168.1.20	192.168.1.20	80	Open	0.000	...
192.168.1.21	192.168.1.21	80	Open	0.000	...
192.168.1.22	192.168.1.22	80	Open	0.000	...
192.168.1.23	192.168.1.23	80	Open	0.000	...
192.168.1.24	192.168.1.24	80	Open	0.000	...
192.168.1.25	192.168.1.25	80	Open	0.000	...
192.168.1.26	192.168.1.26	80	Open	0.000	...
192.168.1.27	192.168.1.27	80	Open	0.000	...
192.168.1.28	192.168.1.28	80	Open	0.000	...
192.168.1.29	192.168.1.29	80	Open	0.000	...
192.168.1.30	192.168.1.30	80	Open	0.000	...
192.168.1.31	192.168.1.31	80	Open	0.000	...
192.168.1.32	192.168.1.32	80	Open	0.000	...
192.168.1.33	192.168.1.33	80	Open	0.000	...
192.168.1.34	192.168.1.34	80	Open	0.000	...
192.168.1.35	192.168.1.35	80	Open	0.000	...
192.168.1.36	192.168.1.36	80	Open	0.000	...
192.168.1.37	192.168.1.37	80	Open	0.000	...
192.168.1.38	192.168.1.38	80	Open	0.000	...
192.168.1.39	192.168.1.39	80	Open	0.000	...
192.168.1.40	192.168.1.40	80	Open	0.000	...
192.168.1.41	192.168.1.41	80	Open	0.000	...
192.168.1.42	192.168.1.42	80	Open	0.000	...
192.168.1.43	192.168.1.43	80	Open	0.000	...
192.168.1.44	192.168.1.44	80	Open	0.000	...
192.168.1.45	192.168.1.45	80	Open	0.000	...
192.168.1.46	192.168.1.46	80	Open	0.000	...
192.168.1.47	192.168.1.47	80	Open	0.000	...
192.168.1.48	192.168.1.48	80	Open	0.000	...
192.168.1.49	192.168.1.49	80	Open	0.000	...
192.168.1.50	192.168.1.50	80	Open	0.000	...
192.168.1.51	192.168.1.51	80	Open	0.000	...
192.168.1.52	192.168.1.52	80	Open	0.000	...
192.168.1.53	192.168.1.53	80	Open	0.000	...
192.168.1.54	192.168.1.54	80	Open	0.000	...
192.168.1.55	192.168.1.55	80	Open	0.000	...
192.168.1.56	192.168.1.56	80	Open	0.000	...
192.168.1.57	192.168.1.57	80	Open	0.000	...
192.168.1.58	192.168.1.58	80	Open	0.000	...
192.168.1.59	192.168.1.59	80	Open	0.000	...
192.168.1.60	192.168.1.60	80	Open	0.000	...
192.168.1.61	192.168.1.61	80	Open	0.000	...
192.168.1.62	192.168.1.62	80	Open	0.000	...
192.168.1.63	192.168.1.63	80	Open	0.000	...
192.168.1.64	192.168.1.64	80	Open	0.000	...
192.168.1.65	192.168.1.65	80	Open	0.000	...
192.168.1.66	192.168.1.66	80	Open	0.000	...
192.168.1.67	192.168.1.67	80	Open	0.000	...
192.168.1.68	192.168.1.68	80	Open	0.000	...
192.168.1.69	192.168.1.69	80	Open	0.000	...
192.168.1.70	192.168.1.70	80	Open	0.000	...
192.168.1.71	192.168.1.71	80	Open	0.000	...
192.168.1.72	192.168.1.72	80	Open	0.000	...
192.168.1.73	192.168.1.73	80	Open	0.000	...
192.168.1.74	192.168.1.74	80	Open	0.000	...
192.168.1.75	192.168.1.75	80	Open	0.000	...
192.168.1.76	192.168.1.76	80	Open	0.000	...
192.168.1.77	192.168.1.77	80	Open	0.000	...
192.168.1.78	192.168.1.78	80	Open	0.000	...
192.168.1.79	192.168.1.79	80	Open	0.000	...
192.168.1.80	192.168.1.80	80	Open	0.000	...
192.168.1.81	192.168.1.81	80	Open	0.000	...
192.168.1.82	192.168.1.82	80	Open	0.000	...
192.168.1.83	192.168.1.83	80	Open	0.000	...
192.168.1.84	192.168.1.84	80	Open	0.000	...
192.168.1.85	192.168.1.85	80	Open	0.000	...
192.168.1.86	192.168.1.86	80	Open	0.000	...
192.168.1.87	192.168.1.87	80	Open	0.000	...
192.168.1.88	192.168.1.88	80	Open	0.000	...
192.168.1.89	192.168.1.89	80	Open	0.000	...
192.168.1.90	192.168.1.90	80	Open	0.000	...
192.168.1.91	192.168.1.91	80	Open	0.000	...
192.168.1.92	192.168.1.92	80	Open	0.000	...
192.168.1.93	192.168.1.93	80	Open	0.000	...
192.168.1.94	192.168.1.94	80	Open	0.000	...
192.168.1.95	192.168.1.95	80	Open	0.000	...
192.168.1.96	192.168.1.96	80	Open	0.000	...
192.168.1.97	192.168.1.97	80	Open	0.000	...
192.168.1.98	192.168.1.98	80	Open	0.000	...
192.168.1.99	192.168.1.99	80	Open	0.000	...
192.168.1.100	192.168.1.100	80	Open	0.000	...

Search screen

  47N R3A

NEW SEARCH

LICENSE PLATE

LOCATION

ADDRESS

RADIUS

OPTIONS

START DATE AND TIME

END DATE AND TIME

LOGIN

INFORMATION

MI OKM

NO PAGING FROM ARCHIVED DATA

SERVERS

- Local
- All Servers
- Long Beach PD
- El Segundo PD
- Burbank PD
- La Verne PD
- Menrovia PD
- Glendora PD
- Torrance PD
- CSU Long Beach PD
- Irwindale PD
- Arcadia PD
- South Pasadena PD
- San Gabriel PD
- Glendale PD
- Beverly Hills PD
- Monterey Park PD
- Sierra Madre PD
- Gardena PD
- Vernon PD
- Hawthorne PD

BOSS: BACK OFFICE SYSTEM SERVER COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

Local: ← All Insd vehicles/sights

All Servers ←

Long Beach PD

El Segundo PD

Burbank PD

La Verne PD

Monrovia PD

Glendora PD

Torrance PD

CSU Long Beach PD

Irwindale PD

Arcadia PD

South Pasadena PD

San Gabriel PD

Glendale PD

Beverly Hills PD

Monterey Park PD

Sierra Madre PD

Gardena PD

Vernon PD

Hawthorne PD

LAPD

Manhattan Beach PD

Pasadena PD

South Gate PD

Search

Outside Agency Servers

The screenshot shows a Microsoft Internet Explorer browser window displaying a search results page for the term 'BOSS'. The search engine used is 'MSN'. The results are sorted by 'Relevance' and show two items:

- Item 1:**
 - Search Results:** BOSS
 - URL:** http://www.fishbase.org/SpeciesSummary.php?Species=BOSS
 - Event(s):** 1
 - Match Results:** 100%
 - Thumbnail:** A small image of a fish.
 - Text:** BOSS
 - Source:** FishBase
- Item 2:**
 - Search Results:** BOSS
 - URL:** http://www.fishbase.org/SpeciesSummary.php?Species=BOSS
 - Event(s):** 1
 - Match Results:** 100%
 - Thumbnail:** A small image of a fish.
 - Text:** BOSS
 - Source:** FishBase

The browser's address bar shows 'http://www.fishbase.org/SpeciesSummary.php?Species=BOSS'. The status bar at the bottom indicates 'Microsoft Internet Explorer'.

Searching a license plate,

NEW SEARCH

LICENSE PLATE

1ABC123

LOCATION

ADDRESS

RADIUS

OPTIONS

MISREADS ONLY

HITS ONLY

START DATE AND TIME

28 ▼ Sep ▼ 2008 ▼ 13 ▼ 42 ▼

END DATE AND TIME

26 ▼ Oct ▼ 2009 ▼ 13 ▼ 42 ▼

Searching a partial license plate.

NEW SEARCH	
LICENSE PLATE	1ABC*
LOCATION	
ADDRESS	
RADIUS	
OPTIONS	MISREADS ONLY <input type="checkbox"/> HITS ONLY <input type="checkbox"/>
START DATE AND TIME	28 Sep 2008 13 42
END DATE AND TIME	26 Oct 2009 13 42

1ABC*
*C123
ABC

1AB_123
1A_C1_3
*ABC_3

Searching by an LASD/ALPR vehicle

NEW SEARCH

LICENSE PLATE

LOCATION

ADDRESS

RADIUS

OPTIONS

MISREADS ONLY HITS ONLY

START DATE AND TIME

28	▼	Sep	▼	2008	▼	13	▼	42	▼
----	---	-----	---	------	---	----	---	----	---

END DATE AND TIME

26	▼	Oct	▼	2009	▼	13	▼	42	▼
----	---	-----	---	------	---	----	---	----	---

Searching an address or area

NEW SEARCH			
LICENSE PLATE	<input type="text"/>		LOGIN
LOCATION	<input type="text"/>		INFORMATION
ADDRESS	12440 E. Imperial Hwy, Norwalk		
RADIUS	<input type="text" value="5.0"/>	<input checked="" type="radio"/> MI	<input type="radio"/> KM
OPTIONS	<input type="checkbox"/> MISREADS ONLY <input type="checkbox"/> HITS ONLY		<input type="checkbox"/> NO PAGING
START DATE AND TIME	<input type="text" value="30"/> <input type="text" value="▼"/> <input type="text" value="Apr"/> <input type="text" value="▼"/> <input type="text" value="2009"/> <input type="text" value="▼"/>	<input type="text" value="12"/> <input type="text" value="▼"/> <input type="text" value="48"/> <input type="text" value="▼"/>	SERVERS
END DATE AND TIME	<input type="text" value="30"/> <input type="text" value="▼"/> <input type="text" value="Jul"/> <input type="text" value="▼"/> <input type="text" value="2009"/> <input type="text" value="▼"/>	<input type="text" value="12"/> <input type="text" value="▼"/> <input type="text" value="48"/> <input type="text" value="▼"/>	<input type="checkbox"/> Local

Searching by date(s)

NEW SEARCH

LICENSE PLATE

LOCATION

ADDRESS

RADIUS

OPTIONS

START DATE AND TIME

END DATE AND TIME

MISREADS ONLY

HITS ONLY

28 ▼ Sep ▼ 2008 ▼ 13 ▼ 42 ▼

26 ▼ Oct ▼ 2009 ▼ 13 ▼ 42 ▼

and times.

NEW SEARCH

LICENSE PLATE

LOCATION

ADDRESS

RADIUS

OPTIONS

START DATE AND TIME

END DATE AND TIME

MISREADS ONLY

HITS ONLY

28	▼	Sep	▼	2008	▼	13	▼	42	▼
----	---	-----	---	------	---	----	---	----	---

26	▼	Oct	▼	2009	▼	13	▼	42	▼
----	---	-----	---	------	---	----	---	----	---

Vertical line on the left side of the page.

Horizontal line at the top right of the page.



Search by station

LOGIN INFORMATION

CAS

MI OKM

NO PAGING FROM ARCHIVED DATA

SERVERS

Local

Search beyond 45 days

Date and time

Vehicle photo



BOSS 47N R3A

- Home
- Report
- Admin
- SYSTEM
- PIPS
- BLANK
- My Profile
- Print
- Sign Out

SELECT	Date and time	Vehicle photo	Description	Code
<input type="checkbox"/>	7/30/2009 12:13:14 PM		LACO WARRANT: LAM9MP07059B1, 29152(A)/VC MISDEMEANOR	VES-34
<input type="checkbox"/>	7/30/2009 11:47:44 AM		STOLEN VEHICLE: CA1920090608	VES-19
<input type="checkbox"/>	7/30/2009 11:22:05 AM		LOST OR STOLEN PLATE: CA1920070330	VES-29
<input type="checkbox"/>	7/30/2009 11:13:14 AM		LOST OR STOLEN PLATE: CA1920090105	VES-33
<input type="checkbox"/>	7/30/2009 10:23:3 AM		LACO WARRANT: P49854919000, 12500A/VC MISDEMEANOR	PLM
<input type="checkbox"/>	7/30/2009 10:22:53 AM		LACO WARRANT: P49854919000, 12500A/VC MISDEMEANOR	PLM
<input type="checkbox"/>	7/30/2009 9:39:38 AM		LACO WARRANT: CG7BF05685D1, 14601.1(A)/VC MISDEMEANOR	CEN
<input type="checkbox"/>	7/30/2009 8:55:08 AM		LOST OR STOLEN PLATE: CA5420080905	CEN

BOSS: BACK OFFICE SYSTEM SERVER

COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

Both license plates

You MUST compare these plates. All hits must be confirmed.

PIPS **BOSS** 47N R3A

Home
Reports
ADMIN
SYSTEM
PIPS
ALARMS
MANAGEMENT
PRINT
Sign Out

LOGIN ID: PLM
CONFIDENCE: 95
TIMESTAMP: 7/30/2009 10:23:36 AM
LOCATION: PLM-M-S07000

34.601925; -118.14427

LAC0 Warrant		\$60,035.00	P49854919000; 12500A/VC MISDEMEANOR
-----------------	--	-------------	---

MAP SATELLITE HYBRID

BOSS: BACK OFFICE SYSTEM SERVER COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

If they do not match, it did not check the data base correctly, but the scanned plate may still be identifiable.

Satellite view

APiPS
BOSS 47N 83W

Location: PEMANANG 807600

GPS: SA 60 925 10011427

SEARCH WARRANT

1248854916000
125004400
MISDEMEANOR

The image shows a satellite view of a building complex, likely a residential or institutional facility, with a grid overlay. The interface includes a search bar at the top with the text 'APiPS BOSS 47N 83W'. Below the search bar, there are several fields: 'Location: PEMANANG 807600', 'GPS: SA 60 925 10011427', and 'SEARCH WARRANT'. To the right of these fields, there are three small boxes containing the numbers '1248854916000', '125004400', and the text 'MISDEMEANOR'. The satellite view itself shows a large building with a central courtyard and several smaller structures. A grid is overlaid on the image, and there are various icons and controls visible around the perimeter of the view.

Deputies in the cars can enter license plates they wish to search for. An example might be a 215 P.C. just occurred.



An investigator can also request the field deputy to enter a plate that they are trying to locate.

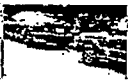







The advantage to a manual entry is that the car's ALPR system is updated immediately and you do not have to wait for the deputy to update at the station through the wireless connection.

Once the field deputy conducts the wireless update, the manual entry is deleted from the radio car and entered into BOSS. It does not update the other vehicles that the vehicle is wanted.

A manual entry in BOSS may look like a scan, but it is not. The difference is that there is no photograph of the scan, the "confidence" number is "100", and the location will be the GPS where the entry was made, (i.e. a Sheriff's station).

A Century deputy manually entered a stolen vehicle they were looking for,

SELECT	6:42:58 AM		LACO WARRANT: PAS8PS6811301, 12500(A)/VC MISDEMEANOR,	CVS
SELECT	7/29/2009 6:42:58 AM		LACO WARRANT: PAS8PS6811301, 12500(A)/VC MISDEMEANOR,	CVS
SELECT	7/29/2009 6:38:13 AM		LOST OR STOLEN PLATE: CA3020070216	ELA
SELECT	7/29/2009 6:35:52 AM		LACO WARRANT: 911916719420, 146011A/VC INFRACTION,	LNK
SELECT	7/29/2009 6:20:58 AM		STOLEN VEHICLE: CA1920090729	CEN
SELECT	7/29/2009 6:11:37 AM		50884 LACO WARRANT: COM9CPD154101, 14601.1(A)/VC MISDEMEANOR,	CEN
SELECT	7/29/2009 6:10:16 AM		LACO WARRANT: COM9CPD154101, 14601.1(A)/VC MISDEMEANOR,	CEN
SELECT	7/29/2009 6:05:02 AM		STOLEN VEHICLE: CA1920090726	LNK
SELECT	7/29/2009 6:03:48 AM		STOLEN VEHICLE: CA1920090726	LNK

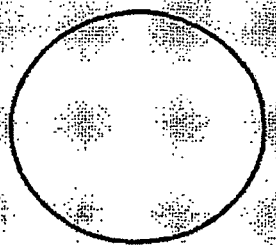
Copyright (C) 2007 BY PIPS TECHNOLOGY, INC.

No vehicle photo

"Confidence" level is "100"



BOSS 47N R3A



LOGIN ID: CEN

CONFIDENCE: 100

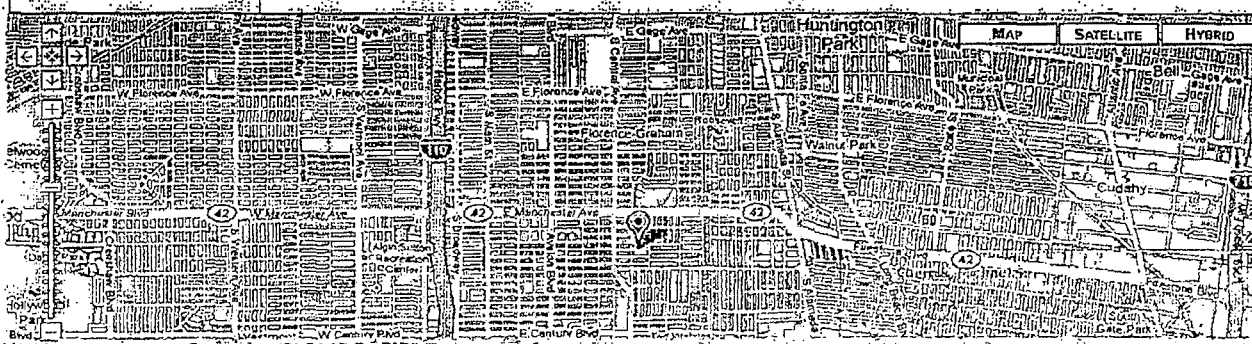
TIMESTAMP: 7/29/2009 6:20:58 AM

LOCATION: CEN-M-SD5837



GPS: 33,95564, -118,253298333333

Stolen Vehicle:	550-B13						CA1920090729
-----------------	---------	--	--	--	--	--	--------------



Copyright (C) 2007 BY PIPS Technology, Inc.

Export Function

Each results page will have an "Export" function link. This will export all relative information from the results page. This can then be entered into an Excel spreadsheet, WORD document, etc

BOSS - Back Office System Server - Microsoft Internet Explorer

Address: http://146.239.6.211:8088/BOSS/GUI/Forms/Default/Default.aspx

BOSS 47N R3A

2007-04-20 08:51:55 PM

Home

Reports

Run Search

Admin/History

Admin

System

PIPS

Admin

My Record

Print

Sign Out

SEARCH RESULTS

(LOCAL)SERVER\RESULTSET

EVENTS (31) EXPORT

MAX RESULTS: 1000

	VLP	TIMESTAMP	OVERVIEW	PATH	INFORMATION
SELECT	[Image]	2007-04-18 12:50:54 PM	[Image]	WITX2S	
SELECT	[Image]	2007-04-18 3:37:22 PM	[Image]	WITX0K	
SELECT	[Image]	2007-04-19 12:29:07 AM	[Image]	[Image]	
SELECT	[Image]	2007-04-21 12:23:29 AM	[Image]	WITL2S	

BOSS: BACK OFFICE SYSTEM SERVER

COPYRIGHT (C) 2007 BY PIPS TECHNOLOGY, INC.

Local Internet

Export Data Pasted into Excel

ALPR data pasted in Excel can be modified and searched for crime analysis

Microsoft Excel - Hills.xls

F1	A	B	C	D	E	G	H	I	J	K	L	M
Read Id	Vrm	LogIn Id	Confidence	Timestamp	Location	Latitude	Longitude	Xaxis	Yaxis	Zaxis	Misread	
15687	5HQ2563	12	98	4/18/2007 1:03	CPT	33.91676667	-118.2060533	-0.392248688	-0.731293893	0.557987975	FALSE	
15692	5HQ2563	12	97	4/18/2007 1:03	CPT	33.91676333	-118.2060483	-0.392248654	-0.731293756	0.557987926	FALSE	
21818	5GSA849	12	92	4/18/2007 18:36	CPT	33.912195	-118.21686	-0.392362037	-0.731272623	0.557921759	FALSE	
21818	5GSA849	12	92	4/18/2007 18:36	CPT	33.912195	-118.21686	-0.392362037	-0.731272623	0.557921759	FALSE	
23104	5VPU722	12	96	4/18/2007 21:10	CPT	33.90325333	-118.2205667	-0.39246795	-0.731325318	0.557792737	FALSE	
23106	5VPU722	12	96	4/18/2007 21:10	CPT	33.90323833	-118.2205833	-0.392468241	-0.731325392	0.55779202	FALSE	
23109	5VPU722	12	97	4/18/2007 21:12	CPT	33.903165	-118.22039	-0.39246871	-0.731326002	0.557790813	FALSE	
23111	5VPU722	12	96	4/18/2007 21:12	CPT	33.90324333	-118.2205633	-0.392468218	-0.73132529	0.557792092	FALSE	
23112	5VPU722	12	100	4/18/2007 20:12	CPT	33.90323667	-118.2205833	-0.39246793	-0.731325518	0.557791996	FALSE	
23114	5VPU722	12	90	4/18/2007 21:13	CPT	33.90323667	-118.22041	-0.39246858	-0.731325164	0.557791996	FALSE	
23114	5VPU722	12	90	4/18/2007 21:13	CPT	33.90323667	-118.22041	-0.39246858	-0.731325164	0.557791996	FALSE	
23495	5XV921	12	97	4/18/2007 22:53	CPT	33.89439833	-118.2266317	-0.39281422	-0.731344641	0.557883958	FALSE	
23800	5FML832	12	97	4/19/2007 0:43	CPT	33.88582333	-118.2659133	-0.393172922	-0.731139188	0.557639722	FALSE	
25354	5VPU722	12	100	4/19/2007 0:51	CPT	33.902965	-118.220445	-0.392470287	-0.731327255	0.557788061	FALSE	
25354	5VPU722	12	100	4/19/2007 0:51	CPT	33.902965	-118.220445	-0.392470287	-0.731327255	0.557788061	FALSE	
25358	5VPU722	12	97	4/19/2007 2:16	CPT	33.90369333	-118.220475	-0.392470079	-0.731325948	0.55778892	FALSE	
25358	5VPU722	12	97	4/19/2007 2:16	CPT	33.90369333	-118.220475	-0.392470079	-0.731325948	0.55778892	FALSE	
25378	1HBN844	12	100	4/19/2007 1:35	CPT	33.90144	-118.22064	-0.392479796	-0.731339	0.557768969	FALSE	
25378	1HBN844	12	100	4/19/2007 1:35	CPT	33.90144	-118.22064	-0.392479796	-0.731339	0.557768969	FALSE	
26417	5GSA849	12	96	4/19/2007 2:44	CPT	33.91223833	-118.2168867	-0.392382178	-0.731272068	0.557922386	FALSE	
26417	5GSA849	12	96	4/19/2007 2:44	CPT	33.91223833	-118.2168867	-0.392382178	-0.731272068	0.557922386	FALSE	
26433	5VPU722	12	96	4/19/2007 2:48	CPT	33.89888667	-118.2075783	-0.392324812	-0.731450368	0.557726981	FALSE	
25433	5VPU722	12	96	4/19/2007 2:48	CPT	33.89888667	-118.2075783	-0.392324812	-0.731450368	0.557726981	FALSE	
25534	5VPU722	12	100	4/19/2007 2:06	CPT	33.90917833	-118.2115167	-0.392327725	-0.731335097	0.557878063	FALSE	
25534	5VPU722	12	100	4/19/2007 2:06	CPT	33.90917833	-118.2115167	-0.392327725	-0.731335097	0.557878063	FALSE	
25636	5VPU722	12	100	4/19/2007 2:08	CPT	33.90922833	-118.2115	-0.392327281	-0.731334782	0.557878788	FALSE	
25636	5VPU722	12	100	4/19/2007 2:08	CPT	33.90922833	-118.2115	-0.392327281	-0.731334782	0.557878788	FALSE	

Ready

The following stat codes are available for ASAP/ALPR:

835-ASAP/ALPR-Mobile

836-ASAP/ALPR-Fixed

837-ASAP-CCTV

838-Gunshot detection

839-ASAP-misc

These stat codes may not be listed in your books. Please include them where possible. Also, any success stories involving ALPR/BOSS can be forwarded to the asapteam@lasd.org.

Email at: ASAPTEAM@LASD.ORG

ASAP

ADVANCED SURVEILLANCE AND PROTECTION

562) 345-4390

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PROOF OF SERVICE

(CCP §§ 1013(a) and 2015.5; FRCP 5)

State of California,)
) ss.
County of Los Angeles)

I am employed in the County of Los Angeles. I am over the age of 18 and not a party to the within action. My business address is 1100 El Centro Street, South Pasadena, California 91030.

On this date, I served the foregoing document described as **DECLARATION OF JOHN GAW IN SUPPORT OF COUNTY OF LOS ANGELES' OPPOSITION TO PETITION FOR WRIT OF MANDAMUS** on the interested parties in this action by placing same in a sealed envelope, addressed as follows:

SEE ATTACHED SERVICE LIST

(BY MAIL) - I caused such envelope(s) with postage thereon fully prepaid to be placed in the United States mail in Orange, California to be served on the parties as indicated on the attached service list. I am "readily familiar" with the firm's practice of collection and processing correspondence for mailing. Under that practice, it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid at Orange, California in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

(BY CERTIFIED MAIL) - I caused such envelope(s) with postage thereon fully prepaid via Certified Mail Return Receipt Requested to be placed in the United States Mail in South Pasadena, California.

BY EXPRESS MAIL OR ANOTHER METHOD OF DELIVERY PROVIDING FOR OVERNIGHT DELIVERY

(BY ELECTRONIC FILING AND/OR SERVICE) - I served a true copy, with all exhibits, electronically on designated recipients listed on the attached Service List on: _____ (Date) at _____ (Time)

FEDERAL EXPRESS - I caused the envelope to be delivered to an authorized courier or driver authorized to receive documents with delivery fees provided for.

(BY FACSIMILE) - I caused the above-described document(s) to be transmitted to the offices of the interested parties at the facsimile number(s) indicated on the attached Service List and the activity report(s) generated by facsimile number (626) 243-1111 indicated all pages were transmitted.

(BY PERSONAL SERVICE) - I caused such envelope(s) to be delivered by hand to the office(s) of the addressee(s).

Executed on **February 21, 2014** at Orange, California.

(STATE) - I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

(FEDERAL) - I declare that I am employed in the office of a member of the bar of this court at whose direction the service was made.

Antonia Mota

ANTONIA MOTA
amota@ccmslaw.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

AMERICAN CIVIL LIBERTIES UNION FOUNDATION, et al. v. COUNTY OF LOS ANGELES, et al.

Case No. BS143004

Our File No. 18623

SERVICE LIST

Peter Bibring, Esq.
ACLU FOUNDATION OF SOUTHERN CALIFORNIA
1313 W. Eighth Street
Los Angeles, CA 90017
(213) 977-9500 – FAX: (213) 977-5299
pbibring@aclu-sc.org
**Attorneys for Petitioners, AMERICAN CIVIL
LIBERTIES UNION FOUNDATION OF SOUTHERN
CALIFORNIA and ELECTRONIC FRONTIER
FOUNDATION**

Jennifer Lynch, Esq.
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333 – FAX: (415) 436-9993
jlynch@eff.org
**Attorneys for Petitioners, AMERICAN CIVIL
LIBERTIES UNION FOUNDATION OF SOUTHERN
CALIFORNIA and ELECTRONIC FRONTIER
FOUNDATION**

Carmen Trutanich, City Attorney
Carlos De La Guerra, Managing Assistant City Attorney
Debra L. Gonzales, Supervising Assistant City Attorney
Heather L. Aubry, Deputy City Attorney
200 North Main Street
City Hall East, Room 800
Los Angeles, CA 90012
(213) 978-8393 – FAX: (213) 978-8787
**Attorneys for Respondents, CITY OF LOS ANGELES
and LOS ANGELES POLICE DEPARTMENT**