October 6, 2011

VIA FIRST CLASS MAIL

Mr. Peter Bibring
ACLU
1313 West Eighth Street
Los Angeles, CA 90017

Re: Public Records Act Request Regarding Surveillance Technologies

Dear Mr. Bibring:

On behalf of the Riverside County Sheriff's Department, this correspondence is in response to your request by the ACLU under the provisions of the California Public Records Act, Government Section 6250 et seq. reference Surveillance Technologies which was received on August 9, 2011.

I have enclosed a copy of your original request for your convenience and reference as I respond to each of the numbered items hereafter.

A. Mobile Phone location records. We hereby request disclosure of all records in your possession relating to seeking or acquiring mobile location records. This request includes but is not limited to records relating to the following:

A1) All policies, procedures, training, and practices related to and/or governing any efforts by the department to obtain mobile location records.

Search warrants are utilized to obtain mobile phone records. Ben Clark Training Center offers three courses on search warrants; Search Warrant Investigators (Search Warrant Preparation), Search Arrest Warrant (Search Warrant Execution), and Advanced Search Warrant. See attached outlines. Course manual is a confidential document and is exempt from disclosure based on Evidence Code 1040(b) (2). See A1 under Attachment A.

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
A2) All policies, procedures, training and practices governing and/or limiting the purposes for which mobile location records are or may be used by the Department.

*There are no responsive records.*

A3) All data retention policies relating to mobile location records, including but not limited to policies detailing how long mobile phone location records are kept, databases in which they are placed, government agencies (federal, state, and local) or non-governmental entities with which they are or they may be shared.

*There are no responsive records.*

A4) The use of mobile location records to identify “communities of Interest” (i.e. those persons who have communicated with a target) in investigations.

*There are no responsive records.*

A5) The use of mobile location records to identify all of the mobile phones at a particular location.

*There are no responsive records.*

A6) The use of “digital fences” (systems by which your agency is notified whenever a mobile phone comes within a specific geographical location).

*There are no responsive records.*

A7) The legal standard of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to obtaining mobile location records.

*The Department follows the legal standard outlined in California Penal Codes section 1525. See A7 under Attachment A.*

A8) Statistics regarding the department’s use of mobile location records, including the number of emergency requests for which no court order was obtained.

*There are no responsive records.*

A9) Any applications by the department to internal or external entities (including but not limited to magistrates or other judicial officers) seeking mobile location records, and any decision or orders ruling on such applications.

*The term "application" is vague and ambiguous, open to multiple interpretations. To the extent you are referring to an application for a search warrant, the Department does not*
have an individual database for tracking search warrant applications. You failed to state a specific timeframe or reasonably identify a record that would enable the Department to search for and identify potentially responsive documents; thus, creating the unreasonable expectation that the Department will examine potentially years worth and potentially thousands of cases and segregate exempt from nonexempt information from a record that is identified as potentially responsive. This request is unreasonable and overly burdensome.

Government code section 6255(a) states that an agency is justified to withhold any record if on the face of the particular case the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record." In American Civil Liberties Union Foundation v. Deukmejian (1982) 32 Cal.3?d 440, the State refused to disclose 100 index "information cards" about criminal defendants and intelligence sources, on the grounds that the inconvenience and burden of reviewing them to distinguish between public and confidential information outweighed the need for disclosure. (Deukmejian, 32 Cal.3?d at 543-454). After examining the records, the court held that "It is clear that the burden of segregating exempt from non-exempt information on the 100 cards would be substantial." (Deukmejian 32 Cal. 3?d at 454).

It is also unknown which search warrant application have become sealed and part of an investigative police file without bifurcating active investigations from those deemed concluded. As clearly set out in Williams v Superior Court (1953) 5 Cal.4?th 337 is the proposition that the investigatory file exemption to the public records act request is not lost even if the investigation is deemed concluded. In addition, particular interests outlive the conclusion of an investigation such as the possibility of endangering the safety of a person involved in the investigation. Williams supra at 357. See also Government Code 6254(f) which exempts law enforcement investigatory files from public disclosure.

Any of the search warrant applications containing intelligence and sealed information would be exempt from public disclosure under 6254(f). See also California Evidence Code section 1040(b) (2) which prevents disclosure of confidential information. For all of the foregoing reasons, the information sought under A9 is denied. However, and in the spirit of cooperation, we kindly direct you to the Riverside Superior Courts where search warrants are maintained and, unless sealed, are open for public viewing. The ACLU staff can make arrangements with the courts for this process.

A10) Communications with mobile companies and providers of location-based services regarding mobile location records, including:

The term "communications" is too broad, vague and ambiguous, and or; open to multiple interpretations. To the extent you are talking about communications designed to gather information for search warrant preparation refer to response A9.

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
Policies and procedures of mobile companies and providers of location-based services regarding release of consumer mobile location records to third-parties, including law enforcement.

*There are no responsive records. The Riverside County Sheriff's Department is not the custodian of these records. The ACLU is capable of contacting each of the mobile phone companies and inquiring as to their individual policies and procedures.*

Requests, court orders or subpoenas sent to mobile companies or providers of location-based services for mobile location records.

*See response to A9.*

Responses by mobile companies and providers of location based services to any such requests, court orders or subpoenas.

*See response to A9.*

Invoices reflecting payments for obtaining mobile location records.

*There are no responsive records.*

Instances in which mobile companies have refused to comply with request or order.

*There are no responsive records. The Riverside County Sheriff Department does not maintain records in instances where mobile phone companies have refused to comply with requests or orders. The ACLU is capable of contacting the mobile phone companies for records of which they are the custodian and request those records.*

B. Internet, Social Network, and Book Service Investigations. We also request disclosure of records in your possession relating to internet investigations, including but not limited to internet investigations utilizing social networking websites or websites providing rental, purchase, borrowing, browsing or viewing of book ("book service sites"). This request includes but is not limited to records relating to the following:

B1) Policies, procedures, and practices governing any efforts by the department to obtain information about suspects, targets of investigations, witnesses or persons of interest through the internet, including through social networking and book service sites.

*There are no responsive records.*

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.*
B2) Training materials provided to department personnel by the department (or by outside trainers contracted by the department) that provide training, guidance or information on how to obtain information about suspects or targets of investigations, witnesses, or persons of interest through the internet, including through social networking and book service sites.

The Department has training related to online internet predators. Actual investigative methods are exempt from disclosure based on evidence code 1040(b) (2). See B2 under attachment B.

B3) Policies, procedures, training, and practices governing and/or limiting the purposes of for which information obtained through the internet, including social networking sites, are or may be used.

There are no responsive records.

B4) Policies, procedures, training and practices governing and/or limiting the sharing of information obtained through the internet, including through social networking sites and book service sites, with other (federal, state and local) government or law enforcement agencies, or non-governmental entities or individuals.

There are no responsive records. However, see California Penal Code section 13300 et. sec., which states criminal offender records shall not be released except as authorized by law. See B4 under Attachment B.

B5) All policies, procedures, training or practices relating to the maintenance and retention of data or information obtained through the internet, including through networking sites, including but not limited to policies detailing how records of such information are kept, databases in which they are placed limitations on who may access the records and for what purposes, and circumstances under which they are deleted.

The Department does not have a policy regarding the retention of information obtained via the internet and/or networking sites. For general records and information retention the Department defaults to the following authorities; County of Riverside General Records Retention Schedule, Riverside County Sheriff’s Department General Orders section 900.00-900.03 and 401.19, Riverside County Sheriff’s Department Dispatch Operations Manual section 601.09, Archival Tapes, County of Riverside Board of Supervisor’s Resolution No. 82-134, Riverside County Sheriff’s Department Directive #11-027 ESI / Civil Litigation and Nelson v. Superior Court (County of Los Angeles) (2001) Cal. App. 4th.

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
Records are shared with law enforcement in accordance with California Penal Code section 13300 et.al. See B5 under Attachment under B.

B6) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to engaging in such investigations.

There are no responsive records. The Internet, Social Networking Sites and Books services are investigative tools that are utilized when the information that may be gleaned from the site is relevant the open investigation. Information accessed is open and available to all users of the World Wide Web. To the extent you are referring to search warrants and court orders refer to A7.

B7) Statistics regarding the department’s use of social networking or book service records, including the number of requests for which no court order was obtained.

There are no responsive records.

B8) Any applications by the department to internal or external entities (including but not limited to magistrate or other judicial officers) seeking social networking or book service records, and any decisions or orders ruling on such applications.

Any responsive documents are exempt from disclosure pursuant to Government Code section 6254(f). Refer to A9. See B8 under Attachment B.

B9) Communications with social networking or book service providers regarding records, including

Too vague and burdensome to research as well as being outside of the scope and control of the Department. Refer to A10.

Policy and procedures of social networking or book service providers regarding release of consumer records to third parties, including law enforcement

There are no responsive records. Refer to A10.

Requests, court orders or subpoenas sent to social networking or book service providers;

Refer to A9.

Responses by social networking or book services providers to any such requests, court orders or subpoenas

Any responsive documents are exempt from disclosure pursuant section 6254(f). Refer to A9. See B8 under Attachment B.

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
Invoices reflecting payments for obtaining social networking or book service records;

There are no responsive records.

Instances in which social networking or book service providers have refused to comply with a request order.

There are no responsive records. The Riverside County Sheriff Department does not maintain records in instances where mobile phone companies have refused to comply with requests or orders. The ACLU is capable of contacting the mobile phone companies for records of which they are the custodian to request those records.

C. GPS Tracking Devices and ALPR. We also request disclosure of records in your possession relating to GPS tracking device or “ALPR”. This request includes but is not limited to records relating to the following;

C1) All records relating to the acquisition, purchase, and deployment of GPS Tracking Devices and/or ALPR’s, including but not limited to all records relating to the number of such devices owned by the department, their location, and the unit or division of the department given primary use of the device.

There are approximately 28 pages of invoices identifying the purchase of and the location of GPS devices dating back to 2007. There are two pages identifying purchases of ALPRs since November 2008. See C1 under attachment C.

C2) All records relating to GPS tracking devices and/or ALPR’s owned or operated by other government agencies (including non-law enforcement) and private entities within the department’s jurisdiction, for which the department can access any or all data collected.

There are no responsive records.

C3) All policies, procedures, training and practices governing use by department of GPS tracking devices and or ALPRS.

There are no responsive records. Case law, reasonable suspicion if vehicle is in a public area, search warrant if vehicle is on private property. Refer to C4.

C4) All training materials provided by to department personnel by the department (or by outside trainers contracted by the department) that provide training, guidance or information in the use of GPS tracking devices or ALPR’s.

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
There are no responsive records. Outside training on generic GPS devices provided by DOJ in a high tech surveillance course, however Riverside County Sheriff's Department is not the custodian of those records. User manuals are provided with the devices and are available to users.

C5) All policies, procedures, training, and practices governing and/or limiting the purposes for which the information obtained through GPS tracking devices and/or ALPR devices may be used by the department or shared with other (federal, state or local) government agencies or non-government agencies.

There are no responsive records. Refer to California Penal Code section 13300 et. sec. See C5 under attachment C.

C6) All data policies relating to the maintenance and retention of information obtained through GPS tracking devices and/or ALPR’s, including but not limited to policies detailing how records of such information are kept, databases in which they are placed, limitations on whom may access the record and for what purpose.

The information gathered by GPS devices are uploaded to the manufacture's website. A supervisor accesses the site and views the information. Information is maintained in the case agent’s case file. Records are maintained to comply with the statute of limitations, appeals process and after a Judge has authorized the destruction of records. Records are shared within the criminal justice system when necessary in the furtherance of an open investigation. Refer to California Penal Code section 13300 et. sec. Refer to General Orders 900-900.08; See C6 under attachment C.

C7) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the Department requires or proffers prior to using GPS tracking devices and/or ALPRs.

There are no responsive records. Refer to A7.

D. Public Video Surveillance cameras/ Facial Recognition Technologies. We also request disclosure of records in your possession relating to the use of Public video Surveillance Cameras and Facial Recognition Technology. The request includes, but is not limited to records relating to the following:

D1) The number and location of public video surveillance cameras currently in the jurisdiction of the Department.

The Department does have security cameras in and around our facilities used primarily for the security of those facilities. According to your footnote #4 on page 5 of your

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
request, we interpret your request to mean surveillance cameras placed in public locations not for the purpose of interior or exterior building security. If that is correct, the Department has no permanent public video surveillance cameras. For special or undercover investigations, the Department uses surveillance video to gather intelligence and evidence pertinent to an assignment and to supplement prosecution. Those records are exempt from public disclosure under Government Code 6254(f). Also see Evidence Code 1040(b) (2) and the aforementioned response to #A9. See D1 under Attachment D.

D2) The number and location of public video surveillance cameras currently There are no public video surveillance cameras.

There are no responsive records.

D3) Which public department or departments control, or will control, the use of public surveillance cameras, and which public or departments have access to, or will have access to, the camera footage and for what purposes.

There are no responsive records.

D4) Policies or procedures regarding the public video surveillance cameras located in the Department’s jurisdiction or planned to be installed in the Department’s jurisdiction, including but not limited to: access to camera footage to the public, the provision of the camera footage, retention of camera footage, purging of the camera footage, the sharing of the camera footage with other agencies, and evaluating the video surveillance camera program.

There are no responsive records.

D5) The use or proposed use of “facial recognition” technology in conjunction with either any public video surveillance cameras or any other video or image data.

The Facial Recognition Technology is utilized by CAL-ID. The facial recognition program searches the Riverside County photograph depository. The depository contains photographs of booking photos from the five jails throughout the county. The facial recognition program makes a comparison and provides the user with a list of possible matches. The user then examines the possible matches and makes a determination if there is a suitable match.

The facial recognition program is only used in ongoing investigations and there for those responsive records are exempt from disclosure based on section 6254(f). See D5 under attachment D.

D6) Programs, policies or procedures(or proposals for programs, policies and procedures) relating to real time access by the department, for law enforcement or

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
other government purposes, to video cameras installed on private property or controlled by private businesses or individuals.

There are no responsive records.

D7) The funding used to purchase existing video surveillance cameras or allocated for the purchase of future cameras, including general funds allocated by local governments, drug forfeiture or other diverted funds, and any applications, proposals, or award letters from federal and state funding sources.

Purchase of two pole cameras utilizing CalMMET funds. See D7 under Attachment D.

D8) The number of times each year for the last five years that the video surveillance camera footage has been requested, by whom and for what purpose.

There are no responsive records.

D9) The number of times each year for the last five years that video surveillance camera footage was used in an investigation of any crime, including the role, if any, it played in identifying or arresting suspects.

There are no responsive records.

D10) Communications from vendors, contracts, specifications, requests for proposals, or other information related to the purchase, installation or technological capabilities of existing public video surveillance cameras or additional video cameras that are being considered for installation in the city. We are requesting all such communications even if the Department does not already have a public video surveillance program.

There are no responsive records.

D11) All records, data, analyses or statistics relating to the effect (or lack thereof)

There are no responsive records.

E. Mobile Forensic Data Extraction- we also request the disclosure of records in your possession relating to the use of technology for the “Mobile Forensic Data Extraction.” This includes but is not limited to the records relating to the following:

E1) The Mobile Forensic Data Extraction devices currently owned by the Department or proposed for purchase by the Department, and the unit or division of the Department given primary use of each device

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
CATCH- One Cellebrite, One Logicube Celdek, Two Susteen DataPilot Systems, Two Susteen SecureView Systems.

Moreno Valley- One Cellebrite

Palm Desert- One Cellebrite

E2) All policies, procedures, training and practices governing use by Department personnel of any such Mobile Forensic Extraction Device.

There are no responsive records in regards to policy. Manufacturer manuals are used as reference materials. Procedures taught by Cal DOJ ATC and other outside computer forensic courses. Department members utilize other law enforcement agencies, device manufacturers and the Internet as additional resources when processing mobile devices.

E3) All policies, procedures, training and practices governing, limiting or relating to the purposes for which Mobile Forensic Data Extraction devices may be used.

There are no responsive records related to policy. As with all digital evidence we conduct exams in the following circumstances; pursuant a search warrant, Fourth Amendment waivers, consent, government owned, and/or found property.

E4) All data policies relating to the maintenance and retention of information obtained through mobile forensic devices, including but not limited to policies detailing how records of such information are kept, databases in which they are placed, limitations on who may access the records and for what purposes, circumstances under which they are deleted, and circumstances under which they may be shared with other government agencies or non-government agencies.

The Department does not have a policy regarding the retention of information obtained via the mobile forensic devices. For general records and information retention the Department defaults to the following authorities; County of Riverside General Records Retention Schedule, Riverside County Sheriff's Department General Orders section 900.00-900.03 and 401.19, Riverside County Sheriff's Department Dispatch Operations Manual section 601.09. Archival Tapes, County of Riverside Board of Supervisor's Resolution No. 82-134, Riverside County Sheriff's Department Directive #11-027 ESI / Civil Litigation and Nelson v. Superior Court (County of Los Angeles) (2001), Cal. App.4th.

Records are shared with law enforcement in accordance with California Penal Code Section 13300 et.al. See E4 under Attachment E.

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
E5) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to using search devices.

Refer to A7.

F. Other surveillance Technology- we also request disclosure of records in your possession relating to the use of other surveillance technology. We request records relating to the following:

F1) The purchase the proposed purchase, request to purchase, or application for funding to purchase all technology and/or devices, other than those specifically enumerated in the Request A through E, designed to accomplish the following:

a. gather and retain information on specific individuals and/or vehicles without a basis to believe they are involved in a particular crime;

There are no responsive records.

b. capture digital information on the location of a person or vehicle;

There are no responsive records.

c. copy and/or intercept electronic data on mobile devices or computers (not including voice transmissions)

There are no responsive records.

F2) All policies, procedures, training and practices related to the use of any devices and/or technology, purchased by the Department as disclosed in response to request F1.

There are no responsive records.

F3) All policies, procedures, training and practices governing, limiting or relating to the purposes for which such devices and/or technology may be used.

There are no responsive records.

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.*
F4) All data policies relating to the maintenance and retention of information obtained through such devices and/or technology, including but not limited to policies detailing how records of such information are kept, databases in which they are placed, limitations on who may access the records and for what purposes, circumstances under which they are deleted, and circumstances under which they may be shared with government agencies or non-governmental entities.

There are no responsive records.

F5) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to using such devices and/or technology.

There are no responsive records.

Thank you for your interest in these records and please do not hesitate to call if you should have any questions.

Cordially,

[Signature]

STAN SNIFF, SHERIFF
Keith Price, Lieutenant
Professional Standards Bureau

SS:KP:lp

*Records relating to the ALPR were previously provided in a response dated November 10, 2008.
August 3, 2011

By United States Mail

Sheriff Stanley Sniff
Riverside County Sheriff's Department
4095 Lemon Street
Riverside, CA 92501

Re: Public Records Act Request Regarding Surveillance Technologies

Dear Sheriff Sniff,

We are troubled by the recent increase in the adoption of surveillance technologies by police departments across California, without appropriate privacy safeguards. A number of cities have implemented or considered implementing programs to conduct video surveillance of public streets, to automatically identify vehicles and their locations, to allow officers to track the location of suspects through mobile phone records or GPS devices without a warrant. These programs pose a significant threat to privacy rights, particularly when policies to guide their use are inadequate or non-existent.

In light of these concerns, the ACLU of Southern California ("ACLU-SC") submits the following request for records in the possession, custody or control of Riverside County Sheriff's Department (the "Department") pursuant to the California Public Records Act, California Government Code §6250 et seq. The Act requires responding agencies to provide a response within ten (10) days of receipt of a request. See Gov. Code §6256. We look forward to your prompt response.

Throughout these requests, the term "records" includes but is not limited to any paper or electronic information, reports, evaluations, memoranda, correspondence, letters, emails, charts, graphs, flyers, meeting agendas and minutes, training materials, diagrams, forms, DVDs, tapes, CDs, notes or other similar materials.
A. **Mobile Phone Location Records.** We hereby request disclosure of all records in your possession relating to seeking or acquiring mobile location records. This request includes but is not limited to records relating to the following:

A1) All policies, procedures, training, and practices related to and/or governing any efforts by the department to obtain mobile location records.

A2) All policies, procedures, training, and practices governing and/or limiting the purposes for which mobile location records are or may be used by the department.

A3) All data retention policies relating to mobile location records, including but not limited to policies detailing how long mobile phone location records are kept, databases in which they are placed, government agencies (federal, state and local) or non-governmental entities with which they are or may be shared.

A4) The use of mobile location records to identify “communities of interest” (i.e., those persons who have communicated with a target) in investigations.

A5) The use of mobile location records to identify all of the mobile phones at a particular location.

A6) The use of “digital fences” (systems whereby your agency is notified whenever a mobile phone comes within a specific geographic area).

A7) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to obtaining mobile location records.

A8) Statistics regarding the department’s use of mobile location records, including the number of emergency requests for which no court order was obtained.

A9) Any applications by the department to internal or external entities (including but not limited to magistrates or other judicial officers) seeking mobile location records, and any decisions or orders ruling on such applications.

A10) Communications with mobile companies and providers of location-based services regarding mobile location records, including

---

1 The term “mobile location records” refers to records obtained from a cell phone, smartphone, or other mobile device by a telecommunications provider and/or provider of location-based services pertaining to the location of a particular phone, including real-time tracking and records regarding historic mobile location information, and also including all available methods of locating mobile devices, such as “cell site,” triangulation, and GPS.

2 The term “policies” throughout this request includes but is not limited to codes, department policies, rules and regulations, bulletins, memoranda, directives, powerpoint presentations, and training materials.
o Policies and procedures of mobile companies and providers of location-based services regarding release of consumer mobile location records to third-parties, including law enforcement;

o Requests, court orders or subpoenas sent to mobile companies or providers of location-based services for mobile location records;

o Responses by mobile companies and providers of location-based services to any such requests, court orders or subpoenas;

o Invoices reflecting payments for obtaining mobile location records;

o Instances in which mobile companies have refused to comply with a request or order.

B. Internet, Social Network, and Book Service Investigations. We also request disclosure of records in your possession relating to internet investigations, including but not limited to investigations utilizing social networking websites or websites providing the rental, purchase, borrowing, browsing, or viewing of books ("book service sites"). This request includes but is not limited to records relating to the following:

B1) Policies, procedures, and practices governing any efforts by the department to obtain information about suspects, targets of investigations, witnesses or persons of interest through the internet, including through social networking and book service sites.

B2) Training materials provided to department personnel by the department (or by outside trainers contracted by the department) that provide training, guidance or information on how to obtain information about suspects, targets of investigations, witnesses, or persons of interest through the internet, including through social networking and book service sites.

B3) Policies, procedures, training, and practices governing and/or limiting the purposes for which information obtained through the internet, including through social networking sites, are or may be used by the department.

B4) Policies, procedures, training, and practices governing and/or limiting the sharing of information obtained through the internet, including through social networking sites and book service sites, with other (federal, state and local) government or law enforcement agencies, or non-governmental entities or individuals.

B5) All policies, procedures, training, or practices relating to the maintenance and retention of data or information obtained through the internet, including
through networking sites, including but not limited to policies detailing how records of such information are kept, databases in which they are placed, limitations on who may access the records and for what purposes, and circumstances under which they are deleted.

B6) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to engaging in such investigations.

B7) Statistics regarding the department’s use of social networking or book service records, including the number of requests for which no court order was obtained.

B8) Any applications by the department to internal or external entities (including but not limited to magistrates or other judicial officers) seeking social networking or book service records, and any decisions or orders ruling on such applications.

B9) Communications with social networking or book service providers regarding records, including

- Policies and procedures of social networking or book services providers regarding release of consumer records to third-parties, including law enforcement;
- Requests, court orders or subpoenas sent to social networking or book service providers;
- Responses by social networking or book service providers to any such requests, court orders or subpoenas;
- Invoices reflecting payments for obtaining social networking or book service records;
- Instances in which social networking or book service providers have refused to comply with a request or order.

C. GPS Tracking Devices and Automatic License Plate Readers. We also request disclosure of records in your possession relating to GPS Tracking Devices or “automatic license plate readers” (“ALPRs”). This request includes but is not limited to records relating to the following:

3 The term “Automatic License Plate Reader” (or “ALPR”) refers to any camera or sensor trained on public roads or thoroughfares, or publicly owned parking lots or structures, that has the capability to scan for vehicles’ license plates and, using optical character recognition or other technology, to convert the image of a license plate into alphanumeric data reflecting the license plate number.
C1) All records relating to the acquisition, purchase, and deployment of GPS Tracking Devices and/or ALPRs, including but not limited to all records relating to the number of such devices owned by the department, their location, and the unit or division of the department given primary use of the devices.

C2) All records relating to GPS Tracking Devices and/or ALPRs owned or operated by other government agencies (including non-law enforcement) and private entities within the Department’s jurisdiction, for which the Department can access any or all data collected.

C3) All policies, procedures, and practices governing use by the department of GPS Tracking Devices and/or ALPRs.

C4) All training materials provided by the department personnel by the department (or by outside trainers contracted by the department) that provide training, guidance or information the use of GPS Tracking Devices and/or ALPRs.

C5) All policies, procedures, training, and practices governing and/or limiting the purposes for which information obtained through use of GPS Tracking Devices and/or ALPRs may be used by the department or shared with other (federal, state or local) government agencies or non-governmental entities.

C6) All data policies relating to the maintenance and retention of information obtained through GPS Tracking Devices and/or ALPRs, including but not limited to policies detailing how records of such information are kept, databases in which they are placed, limitations on who may access the records and for what purposes, and circumstances under which they are deleted.

C7) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to using GPS Tracking Devices and/or ALPRs.

D. Public Video Surveillance Cameras and Facial Recognition Technology. We also request disclosure of records in your possession relating to the use of Public Video Surveillance Cameras and Facial Recognition Technology. This request includes but is not limited to records relating to the following:

D1) The number and location of public video surveillance cameras currently in the jurisdiction of the Department.

---

4 The term “public video surveillance cameras” or “video surveillance cameras” throughout this request refers to cameras placed in public locations that record the activities of members of the public. Through this request, we do not seek information related to red-light cameras, private cameras that are not accessed by city agencies, or cameras in public buildings used primarily for the security of those buildings.
D2) The number and location of public video surveillance cameras currently proposed for installation in the jurisdiction of the Department.

D3) Which public department or departments control, or will control, the use of public video surveillance cameras, and which public department or departments have access to, or will have access to, the camera footage and for what purposes.

D4) Policies or procedures regarding the public video surveillance cameras located in the Department’s jurisdiction or planned to be installed in the Department’s jurisdiction, including but not limited to: access to camera footage, the provision of camera footage to the public, retention of camera footage, purging of camera footage, the sharing of camera footage with other agencies, and evaluating the video surveillance camera program.

D5) The use or proposed use of “facial recognition” technology,\(^5\) in conjunction with either any public video surveillance cameras or any other video or image data.

D6) Programs, policies or procedures (or proposals for programs, policies or procedures) relating to real-time access by the Department, for law enforcement or other government purposes, to video cameras installed on private property or controlled by private businesses or individuals.

D7) The funding used to purchase existing video surveillance cameras or allocated for the purchase of future cameras, including general funds allocated by local government, drug forfeiture or other diverted funds, and any applications, proposals, or award letters from federal and state funding sources.

D8) The number of times each year for the last five years that video surveillance camera footage from the video cameras has been requested, by whom, and for what purpose.

D9) The number of times each year for the last five years that video surveillance camera footage was used in the investigation of any crime, including the role, if any, it played in identifying or arresting suspects.

\(^5\) For purposes of this request, “facial recognition” technology refers to any computerized application intended to automatically identify a person from a digital image, video or video frame from a video source, through computerized comparison of selected facial features from the image and a facial database. For purposes of this request, the term “facial recognition” technology includes, but is not limited to iris recognition and retina scans.
D10) Communications from vendors, contracts, specifications, requests for proposals, responses to requests for proposals, or other information related to the purchase, installation, or technological capabilities of the existing public video surveillance cameras or additional video cameras that are being considered for installation in the city. We are requesting all such communications even if «Department» does not already have a public video surveillance program.

D11) All records, data, analyses or statistics relating to the effect (or lack thereof) of video surveillance cameras on crime rates or rates of clearance for prosecution of crimes.

E. Mobile Forensic Data Extraction. We also request disclosure of records in your possession relating to the use of technology for the “Mobile Forensic Data Extraction.” This request includes but is not limited to records relating to the following:

E1) The number of Mobile Forensic Data Extraction devices currently owned by the Department or proposed for purchase by the Department, and the unit or division of the Department given primary use of each device.

E2) All policies, procedures, training and practices governing use by Department personnel of any such Mobile Forensic Data Extraction devices.

E3) All policies, procedures, training and practices governing, limiting or relating to the purposes for which Mobile Forensic Data Extraction devices may be used.

E4) All data policies relating to the maintenance and retention of information obtained through Mobile Forensic Data Extraction devices, including but not limited to policies detailing how records of such information are kept, databases in which they are placed, limitations on who may access the records and for what purposes, circumstances under which they are deleted, and circumstances under which they may be shared with other government agencies or non-governmental entities.

E5) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to using such devices.

---

For purposes of this request, the term “mobile forensic data extraction” refers devices or technology capable of extracting data (including but not limited to contact lists, call/email history, emails, application data, login information, location history, and other information stored in memory or a hard drive) from mobile phones, smart phones, and GPS units, and other mobile technology. For an example, see http://www.cellbrite.com/forensic-products/forensic-products.html?loc=seg. As used in this request, the term includes both technology that requires the consent and cooperation of the owner of the mobile device and those that do not.
F. **Other Surveillance Technology.** We also request disclosure of records in your possession relating to the use of other surveillance technology. We request records relating to the following:

F1) The purchase, proposed purchase, requests to purchase, or application for funding to purchase all technology and/or devices, other than those specifically enumerated in the Requests A through E, designed to accomplish the following:

   a. gather and retain information on specific individuals and/or vehicles without any basis to believe that they are involved in a particular crime;

   b. capture digital information on the location of a person or vehicle;

   c. copy and/or intercept electronic data on mobile devices or computers (not including voice transmissions)

F2) All policies, procedures, training and practices related to the use of any devices and/or technology purchased by the Department as disclosed in response to request F1.

F3) All policies, procedures, training and practices governing, limiting or relating to the purposes for which such devices and/or technology may be used.

F4) All data policies relating to the maintenance and retention of information obtained through such devices and/or technology, including but not limited to policies detailing how records of such information are kept, databases in which they are placed, limitations on who may access the records and for what purposes, circumstances under which they are deleted, and circumstances under which they may be shared with other government agencies or non-governmental entities.

F5) The legal standard or level of suspicion (e.g. probable cause, reasonable suspicion, relevance) the department requires or proffers prior to using such devices and/or technology.

Because the ACLU Foundation of Southern California is a non-profit public interest organization, we request that you waive any fees that would be normally applicable to a Public Records Act request. See *North County Parents Organization v. Department of Education*, 23 Cal. App. 4th 144 (1994). If, however, such a waiver is denied, we will reimburse you for the reasonable cost of copying. Please inform us in advance if the cost will be greater than $200.
Thank you for your prompt attention to this matter. Please furnish all applicable records to:

Peter Bibring  
ACLU of Southern California  
1313 West Eighth Street  
Los Angeles, CA 90017

If you have questions, please contact me at 213.977.9500 x295 or pbibring@acluc-sc.org.

Sincerely,

[Signature]

Peter Bibring  
Staff Attorney
California Penal Code Section 1525

A search warrant cannot be issued but upon probable cause, supported by affidavit, naming or describing the person to be searched or searched for, and particularly describing the property, thing, or things and the place to be searched.

The application shall specify when applicable, that the place to be searched is in the possession or under the control of an attorney, physician, psychotherapist or clergyman.
I. INTRODUCTION TO SEARCH WARRANTS
   A. Legal requirements
     1. Hero package
     2. Benefits of obtaining a Search Warrant
     3. The "Good Faith" Exception-Leon
   B. Role of Legal Counsel
     1. Jurisdiction
        a. Definitions
        b. Search Warrant
        c. Affidavit
     2. Statutory grounds for issuance
     3. Probable Cause
     4. Informants
   C. Expertise, Training and Experience
     1. Describing the place to be searched
        a. Premises
        b. Vehicles
        c. Persons
        d. Containers or other places
        e. Incomplete description
        f. Address unknown
        g. Use of photographs
     2. Describing the property to be seized
        a. Overbroad description
        b. Sufficiently Specific Description

II. SEARCH WARRANT PREPARATION
   A. Affidavit
     1. Information not contained in the Affidavit
   B. Magistrate
     1. Technical requirements
     2. Questioning by the Magistrate
   C. Service or Execution of the Warrant and it's return
     1. Time limits for service and return
     2. Failure to make timely execution
        a. New Warrant
        b. Resubmission or expired Warrant
D. Forcible Entry
   1. Entry before a Warrant is obtained
      a. Presenting the Warrant to the occupant
      b. Searches and Seizures of persons on the premises
   2. Searching for specific items
      a. Seizing items found in plain view that are not named in the
         Warrant – “The Nexus” rule
      b. Using victims or dogs to aid in the search
      c. Answering the telephone
   3. Oral affidavits and Telephone Search Warrants
   4. Knock and Talk

III. LAW AND LEGAL PROCEDURES

A. Role of an Officer
   1. District Attorney and court
   2. Court proceedings

B. Officer Safety and Operational Planning
   1. Planning
   2. Preparations
      a. Complete fire
      b. Rap sheet
      c. Photographs
      d. Daily Report
      e. Drivers License record
      f. Traits
      g. History of violence
   3. Communication
   4. Manpower

IV. CURRENT INFORMATION / METHODS / RETURNS

A. The place to be searched
   1. Number of persons
   2. Backgrounds
   3. Any threats to police
   4. Firearms, types, locations
   5. Amount or location of contraband
   6. Suspect’s plan in the event of a raid

B. Equipment
   1. Firearms
   2. The entry techniques
   3. The search techniques
   4. The Seizure
   5. The wrap-up
   6. Safety procedures
1. Introduction to Search Warrants.
   A. Class introductions.
      1. Review Case Study of search warrant that resulted in OIS.
   B. Legal requirements pertaining to search warrants.
      1. Review definitions related to search warrants.
      2. Review Search warrant/ Penal Code 1529.
      3. Discuss statutory grounds for the issuance of search warrants.
      4. Discuss/review Magistrate definition related to search warrants.
      5. Review case law pertaining to search warrants.
   C. Alternatives to search warrants and related information.
      1. Affiant/Affidavit defined.
      4. Review case law pertaining to search warrants.
      5. Alternatives to search warrants.
      7. Description requirements related to search warrants.
      8. Newsroom searches.
     11. Legal Standing.
   D. Mechanics of Search Warrant Completion
      1. Search Warrant face page.
      4. Administrative information related to search warrants.
      5. Steps involved in the completion of a search warrant.
      6. Issues to consider related to search warrants.
      7. Additional issues related to search warrants.
2. Review/discuss various copies of search warrant case studies.

A. Search Warrant Case Studies:
   1. 2002 Homicide Case.
   2. 2007-2008 Fraud Case in Riv. County by suspects from Kansas.
   3. 2008-Bank Robbery Case.
   4. 2009-gang related shooting info obtained from My Space website.
   5. 2008 Fraud Case-piggy bank search warrant.
   6. 2006-Gang related case where multiple locations were hit simultaneously.
   7. 2007-Affidavit involving the rape of minor female, by multiple suspects.
   8. 2007-Identity Theft case where search warrant was served in Fresno California.
   9. 1992 Meth Sales case with the use of CRI, suspect killed during the service of the search warrant by officer.
   10. 2001- Affidavit in support of a search warrant for search warrants in the state of Texas-for 1991 homicide case that occurred in the Coachella Valley.
   11. 2007-288 case in the Coachella Valley, search warrant served in San Diego County.
   12. 2008-case La Quinta California case involving a home invasion robbery. This is a Steagald search warrant often times referred to as a Ramey Warrant. It’s a search warrant for the arrest of a suspect at a third parties residence.
   13. 2003-case involving we-tip/citizen information as well as a safety sweep of the residence.

3. Informant Management class.

A. Types of Informants.
   1. Police Officers
   2. Citizen Informants
   3. Reliable Informants
   4. Unreliable informants.

B. Issues to consider in regards to informants.
   1. Case Law.
   2. Departmental Policy.
   3. Supervisory approval.
   4. District Attorney.

C. Information related to informants.
   1. Officer’s use of judgment.
   2. Informant Motivation.
   3. Informant Records.
   4. Department policy.
5. Informant record/packet.
6. Documentation of CI on Search Warrants and Reports.
7. Informant handling dos and don'ts

4. Class room exercise that includes the completion of a search warrant and review by Deputy District Attorney and or Instructor.

5. Class/Instructor Evaluation.