



August 3, 2011

*By United States Mail*

Chief Greg Suhr  
San Francisco Police Dept  
850 Bryant St, #525  
San Francisco, CA 94103

Re: Public Records Act Request Regarding Surveillance Technologies

Dear Chief Greg Suhr:

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 American Civil Liberties Union of California submits the following request for records<sup>1</sup> in the possession, custody or control of your agency (“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.

**A. Mobile Phone Location Records.** We hereby request disclosure of all records in your possession relating to seeking or acquiring mobile location records.<sup>2</sup> This request includes but is not limited to records relating to the following:

<sup>1</sup> 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.

<sup>2</sup> 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.

NANCY PEMBERTON, CHAIRPERSON | SUSAN MIZNER, JAHAN SAGAFI, FARAH BRELYI, ALLEN ASCH, VICE CHAIRPERSONS | DICK GROSBOLL, SECRETARY/TREASURER  
ABDI SOLTANI, EXECUTIVE DIRECTOR | KELLI EVANS, ASSOCIATE DIRECTOR | CHERI BRYANT, DEVELOPMENT DIRECTOR | SHAYNA GELENDER, ORGANIZING & COMMUNITY ENGAGEMENT DIRECTOR  
LAURA SAPONARA, COMMUNICATIONS DIRECTOR | ALAN SCHLOSSER, LEGAL DIRECTOR | MARGARET C. CROSBY, ELIZABETH GILL, LINDA LYE, JULIA HARUMI MASS, MICHAEL RISHER, JORY STEELE, STAFF ATTORNEYS  
ALLEN HOPPER, NATASHA MINSKER, NICOLE A. OZER, DIANA TATE VERMEIRE, POLICY DIRECTORS | STEPHEN V. BOMSE, GENERAL COUNSEL

- A1) All policies,<sup>3</sup> 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
  - 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;
  - Requests, court orders or subpoenas sent to mobile companies or providers of location-based services for mobile location records;
  - Responses by mobile companies and providers of location-based services to any such requests, court orders or subpoenas;

---

<sup>3</sup> 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.

- Invoices reflecting payments for obtaining mobile location records;
- 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.
- B 7) 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.

- B 8) 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.
- B 9) 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”).<sup>4</sup> 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 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.

---

<sup>4</sup> 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.

- C3) All policies, procedures, and practices governing use by the department of GPS Tracking Devices and/or ALPRs.
- 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 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.<sup>5</sup> 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..
- 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

---

<sup>5</sup> 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.

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,<sup>6</sup> 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.
- 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

---

<sup>6</sup> 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.

Extraction.”<sup>7</sup> 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.

**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;

---

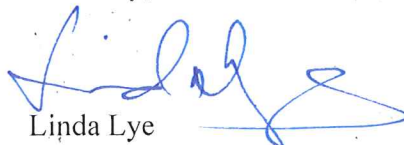
<sup>7</sup> For purposes of this request, the term “mobile forensic data extraction” refers devices or technology capable of extracting data (including but not limited to contact lists, call/email history, emails, application data, login information, location history, and other information stored in memory or a hard drive) from mobile phones, smart phones, and GPS units, and other mobile technology. For an example, see <http://www.cellebrite.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.

- 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 of 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. 4<sup>th</sup> 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 the undersigned at 39 Drumm Street, San Francisco, California 94111. If you have questions, please contact me at (415) 621.2493 or [llye@aclunc.org](mailto:llye@aclunc.org).

Sincerely,



Linda Lye  
Staff Attorney