Item No. 24
Town of Atherton

CITY COUNCIL STAFF REPORT – REGULAR AGENDA

TO: **HONORABLE MAYOR AND CITY COUNCIL**

THROUGH: **GEORGE RODERICKS, CITY MANAGER**

FROM: **STEVEN D. MCCULLEY, CHIEF OF POLICE**

DATE: **SEPTEMBER 20, 2017**

SUBJECT: **RESPONSE TO GRAND JURY REPORT "A DELICATE BALANCE: PRIVACY VS. PROTECTION"**

RECOMMENDATION

Consider the attached response to the San Mateo Grand Jury on their report entitled "A Delicate Balance: Privacy vs. Protection" and, if appropriate, authorize the Mayor to sign the response letter.

BACKGROUND

On July 12, 2017, the San Mateo County Civil Grand Jury released a report entitled "A Delicate Balance: Privacy vs. Protection" (Attachment 1). The purpose of the report is identified as seeking a delicate balance between a community's desire for privacy and the ability of police to protect that same community. Within the report, the Grand Jury developed five findings and three recommendations. The Town of Atherton is required to respond to all findings and recommendations no later than October 10, 2017.

ANALYSIS

The San Mateo County Chiefs' and Sheriff's Association have worked collectively to prepare a response and are aligned with statewide law enforcement organizations including the California Police Chiefs Association, California District Attorneys Association, California State Sheriffs Association, California Peace Officers Association and the Peace Officers Research Association of California (PORAC). In summary, staff agreed with findings of the report. Furthermore, staff determined that partial implementation of the first two recommendations within the report are feasible. However, portions of recommendations one and two, and all of recommendation three, are already addressed by statute. Staff recommends that existing processes that adhere to legislative requirements remain in place.

The attached reply has been prepared for Council consideration and approval. (Attachment 2).

POLICY FOCUS

The Grand Jury requires that the Town indicate agreement or disagreement with specific findings in the Grand Jury Report. Further, the Grand Jury requires that the Town respond to each of the recommendations indicating whether that recommendation has been implemented, will be implemented in the future (with a specific time frame), whether further analysis is needed (with a specific time frame), or whether it will not be implemented.

FISCAL IMPACT

At this time there are no fiscal impacts in response to the Grand Jury.

PUBLIC NOTICE

Public notification was achieved by posting the agenda, with this agenda item being listed, at least 72 hours prior to the meeting in print and electronically. Information about the project is also disseminated via the Town's electronic News Flash and Atherton Online. There are approximately 1200 subscribers to the Town's electronic News Flash publications. Subscribers include residents as well as stakeholders – to include, but be not limited to, media outlets, school districts, Menlo Park Fire District, service providers (water, power, and sewer) and regional elected officials.

ATTACHMENTS

- Grand Jury Report: "A Delicate Balance: Privacy vs. Protection"
- Grand Jury Draft Response letter from Mayor Lempres

A DELICATE BALANCE: PRIVACY VS. PROTECTION

ISSUE

How do local law enforcement agencies in San Mateo County balance their constituents' desire for privacy with the agencies' use of surveillance tools in their efforts to protect the public?

SUMMARY

Finding that delicate balance between a community's desire for privacy and the ability of police and the Sheriff to protect that same community is both a challenge and a necessity. The American Civil Liberties Union (ACLU) states: "Communities must be equal partners in any decision about the use of surveillance technology. They need to know when and why surveillance is being considered, what it is intended to do, and what it will really cost — both in dollars and in individual rights."[1]

Many local police departments and the San Mateo County Sheriff's Office (Sheriff's Office) have purchased or borrowed surveillance tools, such as Automated License Plate Readers (ALPRs). They also use tools, such as in-dash video cameras for patrol cars, body-worn cameras, and ShotSpotter[2] to help them protect residents. These devices can provide evidence to identify and prosecute individuals who commit crimes.

To understand the spread of these new technologies and their impact on communities, the 2016-2017 San Mateo County Civil Grand Jury (Grand Jury) sent a survey to the Sheriff's Office, the Broadmoor Police Protection District, and 17 other law enforcement agencies throughout the County.[3] Survey questions probed for information and details concerning the types of surveillance technology used; policies for collecting, managing, and storing data; and steps taken to ensure public awareness. The Grand Jury also checked whether law enforcement websites posted easily accessible policies for these tools online.

Based on the results of its survey, and its review of policies enacted by various local jurisdictions, the Grand Jury recommends that local law enforcement agencies take additional steps to inform and notify residents when considering plans to purchase and install surveillance technology. Additionally, local law enforcement agencies, and their city councils, should adopt policies and ordinances, with community input, which reflect the communities' desire to balance their safety and privacy. These policies should be posted in a conspicuous place on the agencies' websites.

---

[1] ACLU of Northern California, "Making Smart Decisions about Surveillance: A Guide for community Transparency, Accountability and Oversight," April 2016. https://www.aclunc.org/docs/20160325-making_smart_decisions_about_surveillance.pdf.

[2] Shotspotter is a system that detects and sends the location of gunfire or other weapons using acoustic, optical, or other types of sensors.

[3] Recipients of survey: Sheriff's Office, the Broadmoor Police Protection District, and the law enforcement agencies of the cities and towns of Atherton, Belmont, Brisbane, Burlingame, Colma, Daly City, East Palo Alto, Foster City, Hillsborough, Menlo Park, Millbrae, Pacifica, Redwood City, San Bruno, San Carlos, San Mateo (city), and South San Francisco.

METHODOLOGY

The Grand Jury conducted an extensive survey of police agencies in San Mateo County to determine:

- The types of surveillance technology used in the jurisdiction
- The agency's policies for collecting, managing, and storing surveillance data
- The precautions taken by the agency to ensure public awareness
- Any forthcoming plans by cities or the County for ordinances related to the purchase and deployment of new or borrowed surveillance technology

The Grand Jury also consulted local, state, and federal government websites for background information, and reviewed relevant publications.

GLOSSARY

Automated License Plate Readers (ALPRs): These computer-controlled, high-speed camera systems—generally mounted on police cars or on fixed objects such as light poles—automatically capture an image of every license plate that comes into its view. ALPRs record data on each plate they scan, including not only the plate number but also the precise time, date and place it was encountered.[4]

Body-worn cameras (BWCs): These small cameras worn by law enforcement officers record audio and video. Some types of cameras are always on; other types can be turned on and off by the wearer.

Cell-site simulators: These devices, commonly known as International Mobile Subscriber Identity (IMSI) catchers or "Stingrays," mimic cellphone towers, forcing nearby cellphones into connecting to the device. The cell-site simulator logs the IMSI numbers of cellphones in the area or captures the content of communications.[5]

International Mobile Subscriber Identity (IMSI) catchers: These devices are used in the United States and other countries by law enforcement and intelligence agencies to intercept cellphone traffic and track the movements of cellphone users.

ShotSpotter: These systems detect and send the location of gunfire or other weapons using acoustic, optical, or other types of sensors.

Video surveillance: These camera systems are used to observe and record activities, with or without audio, in public spaces. Live camera feeds can spot crimes in real time, and video recordings can be used in investigations and at trial.

---

[4] "Street-Level Surveillance: Automated License Plate Readers," Electronic Frontier Foundation, accessed May 23, 2017. https://www.eff.org/sls/tech/automated-license-plate-readers.

[5] "Street-Level Surveillance: Cell-site Simulators," Electronic Frontier Foundation, accessed May 23, 2017. https://www.eff.org/sls/tech/cell-site-simulators.

BACKGROUND

Surveillance tools are everywhere: Video cameras are in stores, public buildings, even at a neighbor's front door. Advances in surveillance technology have assisted law enforcement in investigating mass shootings, tracking terrorists, and finding lost children.

As valued as these new surveillance tools are to law enforcement, privacy experts say that innocent people may be targeted.[6] "You have very powerful systems being purchased, most often in secret, with little-to-no public debate and no process in place to make sure that there are policies in place to safeguard community members," said Nicole Ozer, technology and civil liberties policy director for the American Civil Liberties Union (ACLU) of California.[7]

Recent studies show[8] that the public believes it should have a say in how surveillance technology is used. With the issues of privacy and surveillance prominent in the news in recent years, Tulchin Research conducted a California statewide survey[9] in 2015 for the ACLU of California Center for Advocacy and Policy. Tulchin was charged with assessing how likely voters think and feel about criminal justice and law enforcement, including how police use surveillance technology to track Internet, text, email, and other digital activity using handheld devices and computers. Tulchin found that two-thirds of voters would prefer to see local elected officials, such as city council members or county supervisors, approve new surveillance technologies before the devices are deployed (67% support). Similarly, voters want to see policies which set limits on surveillance use both locally (65%) and statewide (64%). The survey also indicated that voters want accountability from law enforcement agencies regarding the frequency of use of surveillance technologies (62%). The public also wants public notification before the purchase of new surveillance technologies (58%).[10]

Public opinion in the Bay Area on surveillance

Although the Grand Jury did not find any surveys of public opinion in San Mateo County on surveillance issues, the balancing of protection vs. privacy has been a subject of interest in the Bay Area.

In 2015, The Center for Investigative Reporting[11] and three local artists[12] collaborated on the arts and journalism project "Eyes on Oakland."[13] The reporters and the artists visited neighborhoods across the city of Oakland informing residents about surveillance technology. Hundreds of residents participated by completing questionnaires. Participants were asked to respond to the prompt: "Surveillance is…"

---

[6] Marisa Kendall, "Surveillance in Silicon Valley is hard to avoid," *San Jose Mercury News*, February 9, 2017. http://www.mercurynews.com/2017/02/09/surveillance-in-silicon-valley-whos-watching-you/.

[7] Ibid.

[8] For information about Tulchin Research, go to http://www.tulchinresearch.com.

[9] See Appendix B.

[10] Tulchin Research, "California Statewide Survey Finds Voters Concerned about Privacy and Want to See Reforms Made to Surveillance Technology Use by Law Enforcement," August 21, 2015, http://www.aclunc.org/docs/20150821-aclu_surveillance_privacy_polling.pdf.

[11] For information about The Center for Investigative Reporting, go to https://www.revealnews.org/, accessed May 23, 2017.

[12] Aaron McKenzie, Chris Treggiari and Peter Foucault

[13] For information on the "Eyes on Oakland" project, go to http://eyesonoakland.tumblr.com/, assessed June 8, 2017.

Here is a sampling of the responses:

- Surveillance is: questionable
- Surveillance is: important
- Surveillance can be used against a peaceful public
- Surveillance is: Technology run amok. Just because we can do it, should we do it?
- Surveillance is: Everywhere. Privacy is a myth in the digital era
- Surveillance is: State violence
- Surveillance is: Not a solution to the systemic problems that create crime and violence. Surveillance No! Education, Equity and Respect, Yes!
- Surveillance is: Great!!! Bring it on. It's for my safety, your safety. Nothing to hide[14]

Privacy advocates have pointed out the impact that surveillance technology may have on residents: "Our concerns stem from the fact that license plate readers can scan and collect the information of innocent people, innocent drivers," said Chris Conley, a policy attorney with the ACLU of Northern California. "Location information can reveal very sensitive information about people. If they're visiting a church, or a clinic or even open-mic night at a bar, all of these things reveal information about a person that shouldn't be sitting in a database somewhere."[15]

Case in point: One San Leandro resident's eye-opening experience

After learning that the city of San Leandro had purchased an ALPR for its Police Department in 2008, computer security consultant Michael Katz-Lacabe asked city officials to send him a record of every instance the scanners photographed his car.

An article on sfgate.com describes what Mr. Katz-Lacabe learned:

> The results shocked him.
>
> The paperback-size device, installed on the outside of police cars, can log thousands of license plates in an eight-hour patrol shift. Katz-Lacabe said it had photographed his two cars on 112 occasions, including one image from 2009 that shows him and his daughters stepping out of his Toyota Prius in their driveway.
>
> That photograph, Katz-Lacabe said, made him "frightened and concerned about the magnitude of police surveillance and data collection." The single patrol car in San Leandro equipped with a plate reader had logged his car once a week on average, photographing his license plate and documenting the time and location.[16]

---

[14] Cole Goins, "What Oakland, California, residents think about police surveillance," *Reveal from the Center for Investigative Reporting*, August 18, 2015. https://www.revealnews.org/article/what-oakland-california-residents-think-about-police-surveillance/.

[15] Samantha Weigel, "Who's watching who?: License plate readers used throughout San Mateo County," *The Daily Journal*, April 8, 2015. http://www.smdailyjournal.com/articles/lnews/2015-04-08/whos-watching-who-license-plate-readers-used-throughout-san-mateo-county/1776425141346.html

[16] Ali Winston, "License plate readers tracking cars," *SFGate*, June 25, 2013. http://www.sfgate.com/bayarea/article/License-plate-readers-tracking-cars-4622476.php.

Legislation

The California Constitution provides for a citizen's right to privacy.[17] State lawmakers are addressing this right as it relates to surveillance systems. In 2015, California lawmakers passed two laws concerning surveillance.[18]

- **SB 741 (2015) Mobile Communications: Privacy[19]**
  "Cell-site simulators," sometimes called International Mobile Subscriber Identity (IMSI) catchers or Stingrays, trick cellphones into connecting to them as they would to a local cellphone tower. This connection enables the simulator to capture an IMSI number (a unique number used to identify a user on the cellular network), the current location, and perhaps the content of the conversation. In general, law enforcement uses cell-site simulators to locate known suspects. A cell-site simulator casts a wide net, collecting all the IMSI numbers in an area until it locates the IMSI number that law enforcement is searching for. Also swept up are the location and IMSI numbers of all cellphones that happen to be nearby.[20]

  Effective January 1, 2016, SB 741, written by Senator Jerry Hill, D – San Mateo, imposes restrictions and requirements on data collected by cell-site simulators and how those data are managed and shared. According to the Electronic Frontier Foundation,[21] any public agency using a cell-site simulator must:
  - Secure and protect the collected data from "unauthorized access, destruction, use, modification, or disclosure."[22]
  - Adopt a usage and privacy policy that is "consistent with respect for any individual's privacy and civil liberties."[23]
  - Obtain approval of the legislative body (for example, the City Council) to acquire such systems and alert the community about the device through a public process. This requirement does not apply to Sheriff's Offices, which must instead provide public notice online that they have acquired such devices.[24]

  Note: None of the respondents to the Grand Jury's survey currently use or have plans to acquire a cell-site simulator.

---

[17] California Constitution, Section 1. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CONS&division=&title=&part=&chapter=&article=I.

[18] ACLU of Northern California *Making Smart Decisions about Surveillance: A Guide for community Transparency, Accountability and Oversight.* April, 2016, 8-9. https://www.aclunc.org/docs/20160325-making_smart_decisions_about_surveillance.pdf

[19] California Government Code Section 53166.

[20] Stephanie LaCambra, "Congressional Oversight Committee Wants to Rein in Police Abuse of Cell-Site Simulators," *Electronic Frontier Foundation DeepLinks* (blog). https://www.eff.org/deeplinks/2017/02/bipartisan-congressional-oversight-committee-wants-probable-cause-warrants-0.

[21] David Maass, "Success in Sacramento: Four New Laws, One Veto—All Victories for Privacy and Transparency," accessed June 2, 2017. https://www.eff.org/deeplinks/2015/10/success-sacramento-four-new-laws-one-veto-all-victories-privacy-and-transparency.

[22] Ibid.

[23] Ibid.

[24] Ibid.

- **SB 34 (2015) Automated License Plate Recognition Systems: Use of Data[25]**
  Effective January 2, 2016, SB 34, also authored by Senator Jerry Hill, D – San Mateo, requires agencies that collect data using ALPRs or access ALPR data to publish their privacy and usage policies. Specifically, such policies shall be available to the public in writing, and, if the ALPR operator has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site.[26]

  In a 2015 *San Jose Mercury News* article,[27] Senator Hill told reporters that approximately 60 law enforcement and public safety agencies in California were using ALPRs. At that time, however, only 8 of the agencies asked for public comment and only 16 published their ALPR policies for review by the public. Hill said agencies must "…have a policy in place on how they're going to use it, what they're going do with the info and how secure it will be. Today there is none of that."[28]

  According to an analysis of the law by the Electronic Frontier Foundation, cities and counties using ALPRs are now required to provide this information:[29]

  - The authorized purposes for using the ALPR system and collecting ALPR information.
  - A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system, or to collect ALPR information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors.
  - A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
  - The purposes of, process for, and restrictions on the sale, sharing, or transfer of ALPR information to other persons.
  - The title of the official custodian, or owner, of the ALPR system responsible for implementing this section.
  - A description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors.
  - The length of time ALPR information will be retained and the process the ALPR operator will utilize to determine if and when to destroy retained ALPR information.[30]

---

[25] California Civil Code sections 1798.29, 1798.82, and 1798.90

[26] California Civil Code section 1798.90.51

[27] Tracy Seipel and Eric Kurhi, "California Digital Privacy Laws Boosted Protecting Consumers from Big Brother, Big Business."

[28] Ibid.

[29] "California Automatic License Plate Reader Policies," Electronic Frontier Foundation, accessed March 30, 2017. https://www.eff.org/pages/california-automated-license-plate-reader-policies.

[30] California Civil Code, sec. 1798.90.51

Note: Nine of the respondents to the Grand Jury's survey currently use or have borrowed ALPRs.

DISCUSSION

The 2016-2017 San Mateo County Civil Grand Jury (Grand Jury) surveyed 19 local law enforcement agencies[31] regarding their surveillance technology. The survey questions addressed these topics:

- Types of surveillance technology used in the jurisdiction
- Policies for collecting, managing, and storing surveillance data
- Precautions taken to ensure public trust
- Proposals made for a local ordinance related to the purchase and deployment of new or borrowed surveillance technology

With the exception of Broadmoor,[32] Colma, and Millbrae, every city and town responding to the Grand Jury survey uses some form of surveillance technology. The devices range from video cameras in police stations to more sophisticated tools, such as ALPRs. The San Mateo County Sheriff's Office uses ALPRs and ShotSpotter.

A closer look: Policies for BWCs and ALPRs

The 2015-16 Grand Jury investigated and reported on body camera usage in the County.[33] At the time that report was written, five police departments used body worn cameras (BWCs): Atherton, Belmont, Foster City, Hillsborough and Menlo Park. Today, 14 police departments and the Sheriff's Office use BWCs, have purchased, or plan to implement them. Currently, Menlo Park is the only law enforcement agency in this group with a policy statement relating to the use of BWC available online.

---

[31] Recipients of survey: Sheriff's Office, the Broadmoor Police Protection District, and the police departments of the cities and towns of Atherton, Belmont, Brisbane, Burlingame, Colma, Daly City, East Palo Alto, Foster City, Hillsborough, Menlo Park, Millbrae, Pacifica, Redwood City, San Bruno, San Carlos, San Mateo (city), and South San Francisco.

[32] Broadmoor Police Protection District used BWCs for a six-month period (with voluntary participation by officers).

[33] San Mateo County Civil Grand Jury 2015-16, "Body Cameras—The Reel Issue," https://www.sanmateocourt.org/documents/grand_jury/2015/body_camera.pdf.

City/Jurisdiction	When Implemented	Expected Implementation	Policy Available Online?
Foster City	2012		Contact Police Department for policy*
Atherton	Prior to 2016		Contact Police Department for policy*
Belmont	Prior to 2016		Contact Police Department for policy*
Hillsborough	Prior to 2016		Contact Police Department for policy*
Menlo Park	Prior to 2016		Policy available online, in Menlo Park Police Department Policy Manual†

Implementation Coming This Year‡			
San Bruno		6/17¶	Not applicable
South San Francisco		7/17¶	Not applicable
Sheriff		10/17‡	Not applicable
Brisbane		10/17‡	Not applicable
Burlingame		10/17¶	Not applicable
Colma		10/17¶	Not applicable
Pacifica		10/17‡	Not applicable
San Mateo		10/17‡	Not applicable
Redwood City		12/17¶	Not applicable
East Palo Alto		Fiscal Year 2017-2018‡	Not applicable

No Plans to Purchase BWCs			
Broadmoor			
Daly City			

*San Mateo County Grand Jury 2015-2016, "Body Cameras—The Reel Truth,". https://www.sanmateocourt.org/documents/grand_jury/2015/body_camera.pdf.

†Menlo Park Police Department Policy Manual Policy 450, accessed May 31, 2017. https://www.menlopark.org/950/Department-policies.

‡San Mateo County Grand Jury 2016-2017, "Summary of Responses to the 2015-2016 San Mateo County Civil Grand Jury Final Reports." https://www.sanmateocourt.org/documents/grand_jury/2016/2015-2016Summary.pdf

¶San Mateo County Grand Jury 2016-2017, "Summary of Responses to the 2015-2016 San Mateo County Civil Grand Jury Final Reports, (Second Summary)." As of June 6, 2017, this report is not yet available online.

Survey results revealed that 9 of 19 law enforcement agencies queried in San Mateo County either own or have temporarily borrowed ALPRs. The Grand Jury reviewed the websites of those nine agencies to determine whether they were in compliance with California Civil Code, sec. 1798.90.51, which was added pursuant to SB 34. Section 1798.90.51 requires that "The usage and privacy policy shall be available to the public in writing, and, if the ALPR operator has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site."[34]

The Grand Jury found as follows:

Law Enforcement Agency	ALPR Policy Conspicuously Placed?
Sheriff	Yes. However, the link to the policy is labeled "ALPR Policy." County residents may not be familiar with the acronym.
Burlingame	No. Policy is not available on website. Burlingame does not own ALPRs, but has used the equipment on an ad hoc basis in connection with specific investigations. If an agency temporarily borrows an ALPR, it is still required to provide a link on its website to a policy statement. No such policy statement is available on the Burlingame police department website.
Daly City	Yes.
Hillsborough	No. Policy is available on the website but not located in a conspicuous place. To find the policy requires searching the website or reading through a long list of FAQs.
Menlo Park	No. Policy is available on the website but not located in a conspicuous place. To find the policy requires searching through the online Police Department Policy Manual.
San Bruno	Yes.
San Carlos	No. Policy is not available on the website.[35]
San Mateo	Yes.
South San Francisco	Yes.

[34] California Civil Code, sec. 1798.90.51

[35] The City of San Carlos purchased the ALPRs but the Sheriff's Office provides police services to the city and operates the vehicle with the ALPR equipment. No link to an ALPR policy is on the San Carlos Police Bureau webpage, nor does that page direct the public to the Sheriff's Office website for the ALPR policy.

In San Mateo County, all law enforcement agencies send the data they collect from ALPRs to the Northern California Regional Intelligence Center (NCRIC).[36] Congress established the NCRIC in 2007, after the Bay Area was designated a high intensity drug trafficking region.[37] NCRIC's reach extends from Monterey County to Del Norte County,[38] covering 15 counties in California.[39] NCRIC is known as an "intelligence fusion center" which, according to the Department of Homeland Security, "...operate[s] as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal, state, local, tribal, territorial (SLTT), and private sector partners."[40]

Access to the NCRIC[41] data is strictly regulated insofar as only law enforcement personnel who meet these criteria may use the database:

- Have agreed to the NCRIC privacy policy and non-disclosure agreement
- Can provide a criminal case or incident name/number
- Have a lawful purpose with a "need to know"[42] and a "right to know"[43] the information.

One common use of APLRs is to compare the license plate numbers collected against a "hot list." This list contains the license plate information of vehicles associated with active investigations, such as Amber Alerts, missing persons, stolen vehicles, or stolen license plates.[44]

---

[36] Samantha Weigel, "Who's watching who?: License plate readers used throughout San Mateo County," *The Daily Journal*, April 8, 2015. http://www.smdailyjournal.com/articles/lnews/2015-04-08/whos-watching-who-license-plate-readers-used-throughout-san-mateo-county/1776425141346.html

[37] "How the NCRIC was Established," NCRIC Northern California Regional Intelligence Center, accessed April 19, 2017..https://ncric.org/default.aspx?MenuItemID=122&MenuGroup=NCRIC+Public+Home&AspxAutoDetectCookieSupport=1

[38] Ibid.

[39] Del Norte, Humboldt, Mendocino, Lake, Napa, Sonoma, Marin, San Francisco, Contra Costa, San Mateo, Alameda, Santa Cruz, Santa Clara, San Benito, Monterey Counties. See a map here of the area here: https://ncric.org/default.aspx?menuitemid=633&menugroup=NCRIC+Public+Home, accessed May 18, 2017.

[40] "State and Major Urban Area Fusion Centers," U.S. Department of Homeland Security, accessed March 30, 2017. https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

[41] NCRIC Northern California Regional Intelligence Center. "Frequently Asked Questions," https://ncric.org/html/ALPR-FAQ-Feb-2015.pdf, accessed May 17, 2017.

[42] According to the NCRIC "Frequently Asked Questions," *Need to know* "...is established when the requested information is pertinent and necessary to the requesting agency in initiating, furthering, or completing the performance of a law enforcement activity.
https://ncric.org/html/ALPR-FAQ-Feb-2015.pdf, accessed May 18, 2017.

[43] According to the NCRIC "Frequently Asked Questions, *Right to know* "...is established when the requester is acting in an official capacity and has statutory authority to obtain the information being sought."
https://ncric.org/html/ALPR-FAQ-Feb-2015.pdf, accessed May 18, 2017.

[44] "NCRIC ALPR FAQs,"
https://ncric.org/html/ALPR-FAQ-Feb-2015.pdf, accessed May 18, 2017.

According to *The Daily Journal*, ALPRs in San Mateo County, and Northern California generally, collect massive amounts of data:[45]

- In a 12-hour shift, one of the City of San Mateo's two ALPR-equipped patrol cars accumulated nearly 10,000 images from four cameras mounted on the roof of the cars (even in the dark).[46]
- In one year, NCRIC amassed around 46.5 million images from its partner agencies.[47]

The data are purged every 12 months, except for those records connected to a crime, which can be held for up to five years.

Law enforcement places a high value on the amount and quality of the data they collect from the ALPRs. For example, San Mateo Police Chief Susan Manheimer informed the *Daily Journal*: "I can't overestimate how important it really is. They're not looking at them for collecting data to know where our neighbors travel, we're specifically looking for cars involved in specific crimes."[48]

As the Grand Jury discovered, seven of the nine County law enforcement agencies using ALPRs have a link on their websites to a policy statement. This policy, in all cases, with the exception of Menlo Park, is a boilerplate statement provided by NCRIC.[49] The information in this generic document does not really provide the level of detail that would be helpful to someone looking for specific information. For instance, the law states that the policy shall include:

> (E) The title of the official custodian, or owner, of the ALPR system responsible for implementing this section."[50]

The NCRIC policy provides the following information regarding "custodians":[51]

> **Custodian of Records and Records Requests**
>
> Each agency operating ALPR technology retains control and ownership as the official custodian of its records, and must independently verify all external information obtained via NCRIC Information Systems. To the extent permitted by law, requests for information under the California Public Records Act or similar applicable laws will be directed back to the owner of the requested data.

The City of San Mateo Police Department's website provides an example of a well-executed and well-publicized policy in this regard. The police department currently uses ALPRs and, in addition to a link to the NCRIC policy statement, its website provides helpful information for

---

[45] Samantha Weigel, "Who's watching who?: License plate readers used throughout San Mateo County," *The Daily Journal*, April 8, 2015. http://www.smdailyjournal.com/articles/lnews/2015-04-08/whos-watching-who-license-plate-readers-used-throughout-san-mateo-county/1776425141346.html

[46] Ibid.

[47] Ibid.

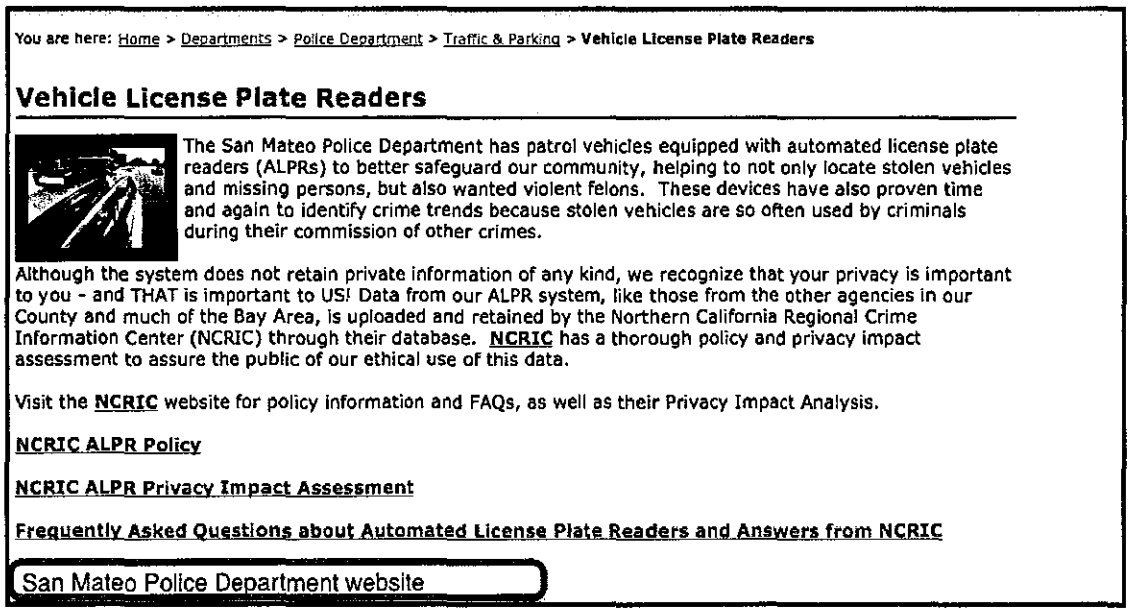
[48] Ibid.

[49] See Appendix A for text of "NCRIC Automated License Plate Reader Policy."

[50] California Civil Code, sec. 1798.90.51

[51] NCRIC, "NCRIC Automated License Plate Reader Policy. "https://ncric.org//html/NCRIC%20ALPR%20POLICY.pdf.

residents wanting to learn about how ALPRs are used in the city.[52] The explanation of the City of San Mateo's use of ALPRs and links to background information, such as the answers to frequently asked questions help those not in law enforcement to better understand the purpose of ALPRs.



You are here: Home > Departments > Police Department > Traffic & Parking > **Vehicle License Plate Readers**

Vehicle License Plate Readers

The San Mateo Police Department has patrol vehicles equipped with automated license plate readers (ALPRs) to better safeguard our community, helping to not only locate stolen vehicles and missing persons, but also wanted violent felons. These devices have also proven time and again to identify crime trends because stolen vehicles are so often used by criminals during their commission of other crimes.

Although the system does not retain private information of any kind, we recognize that your privacy is important to you - and THAT is important to US! Data from our ALPR system, like those from the other agencies in our County and much of the Bay Area, is uploaded and retained by the Northern California Regional Crime Information Center (NCRIC) through their database. **NCRIC** has a thorough policy and privacy impact assessment to assure the public of our ethical use of this data.

Visit the **NCRIC** website for policy information and FAQs, as well as their Privacy Impact Analysis.

NCRIC ALPR Policy

NCRIC ALPR Privacy Impact Assessment

Frequently Asked Questions about Automated License Plate Readers and Answers from NCRIC

San Mateo Police Department website

Interacting with the Community and Building Trust

According to the Grand Jury survey results, the only opportunity that residents may have to comment on the desirability of surveillance technology is at city council meetings. This table shows the responses to the question: "Before purchasing the technology, did you inform residents of your intention to acquire surveillance tools?"[53] Respondents listed the types of interactions they used to connect with community members.

City	Response†
Atherton Burlingame Daly City East Palo Alto Hillsborough Menlo Park Pacifica Redwood City San Bruno San Carlos San Mateo South San Francisco	City or Town Council meetings, staff reports posted on city website

[52] "Vehicle License Plate Readers," San Mateo Police Department, accessed May 6, 2017. http://www.cityofsanmateo.org/index.aspx?nid=3211.

[53] For the actual survey responses to the question "Before purchasing the technology, did you inform residents of your intention to acquire surveillance tools?" see Appendix C.

City	Response†
East Palo Alto Hillsborough Menlo Park Redwood City San Carlos Sheriff's Office	Public meetings, Town Halls
Menlo Park*	Social media
Brisbane Foster City	Did not reach out to residents

* Colma, Pacifica, and South San Francisco stated in the survey that in the future they would use social media to inform residents.

†Some cities stated they did not reach out to residents (Brisbane and Foster City). Belmont responded that the city did reach out, but did not provide any examples. Broadmoor Police Protection District, Colma, and Millbrae currently use surveillance tools, so this question did not apply to them.

Planning by cities or the County to introduce ordinances to manage surveillance technology

According to the Grand Jury survey, neither the County nor any cities in San Mateo County are currently considering an ordinance that outlines processes and procedures for deploying and managing surveillance tools.

Other Bay Area responses to community concerns about surveillance

Oakland Domain Awareness Center (DAC)

In 2013, the City of Oakland was building the DAC system, a large surveillance system comprising 700 cameras placed in schools and public housing, with facial recognition software, ALPRs, and 300 terabytes of storage.[54] In response, a coalition of activists alerted the community to the potential harm widespread surveillance could do to privacy and civil liberties. At city council meetings, speaker after speaker voiced concerns about surveillance technology and requested participation in the decision-making process.[55]

As a result, in 2014, the Oakland City Council voted to confine the DAC surveillance to the Port of Oakland. The council also prohibited use of facial recognition software, ALPRs, and eliminated data retention. The council also created an ad hoc citizen's committee, which later became Oakland's Privacy Advisory Commission.[56] Recently, this commission has proposed a "Surveillance and Community Safety Ordinance,"[57] which would require the city's departments to disclose any new surveillance technologies they plan to acquire. Agencies would need approval from the City Council before purchasing the tool or technology. The law would require open public hearings, to allow the public to evaluate the costs and benefits of technologies before

[54] Brian Hofer, "How the fight to stop Oakland's Domain Awareness Center Laid the Groundwork for the Oakland Privacy Commission," *ACLU of Northern California* (blog), accessed Sept. 21, 2016. https://www.aclunc.org/blog/how-fight-stop-oaklands-domain-awareness-center-laid-groundwork-oakland-privacy-commission.

[55] Ibid.

[56] Ibid.

[57] Text of proposed ordinance, accessed May 6, 2017: https://www.documentcloud.org/documents/3253520-oak061975.html.

they are deployed. Unanimously approved by the commission, the ordinance was pending before the Oakland City Council as of June 6, 2017.[58]

Santa Clara County's surveillance technology and community safety ordinance

In September 2016, Santa Clara County passed an ordinance to protect residents' right to privacy from intrusive and invasive technologies.[59] This ordinance also addresses emerging surveillance tools not yet created. According to the *San Jose Mercury News*:

> The ordinance is aimed at protecting the public's right to privacy from existing and emerging technologies, such as drones, license plate readers, cell phone trackers or things that haven't yet been realized outside of science fiction.
>
> The new rules require that agencies put in place public policies regarding the use of any surveillance technology before it is acquired or activated, and issue annual reports on how the technologies have been used and what they discovered.[60]

Santa Clara County Supervisor Joe Simitian began advocating for an ordinance in 2014, in response to local law enforcement purchasing surveillance technology without informing the public. He became more concerned about the lack of transparency when he learned that San Jose police had purchased a drone and of Oakland's plan to extend the powers of the DAC beyond the Port of Oakland.[61] When the Santa Clara County Sheriff's Office received a grant to buy a $500,000 "Stingray" cell-site simulator, Simitian, backed by many County residents, requested more information about this technology. A press release issued by Simitian's office stated:

> Under the new law, officials who want to purchase and use surveillance technology in Santa Clara County will have to:
>
> - Provide analysis of the privacy and due process implications of the technology they wish to acquire,
> - Submit, for approval, a set of "use policies" governing the use of the technology, before the technology is acquired or used; and,
> - Report back annually on the use of the technology, in order to provide some measure of accountability.
>
> Simitian noted, "for years and years we've made budget allocations without asking the most basic of questions: What information are we collecting? About whom? Why? How

---

[58] Darwin BondGraham, "Oakland Privacy Commission Approves Surveillance Transparency Oversight Law," *East Bay Express,* Jan 6, 2017.
http://www.eastbayexpress.com/SevenDays/archives/2017/01/06/oakland-privacy-commission-approves-surveillance-transparency-and-oversight-law.
Link to proposed ordinance, accessed May 6, 2017: https://www.documentcloud.org/documents/3253520-oak061975.html.
https://occupyoakland.org/wp-content/uploads/2017/01/OPAC-Surveillance-Ordinance-Adopted.pdf.

[59] Ordinance no. NS-300.897 "An Ordinance of the Board of Supervisors of the County of Supervisors of the County of Santa Clara Adding Division A40 of the County of Santa Clara Ordinance code Relating to Surveillance-Technology and Community Safety," accessed May 6, 2017. https://assets.documentcloud.org/documents/2854213/Attachment-149330.pdf.

[60] Eric Kurhi "Pioneering spy-tech law adopted by Santa Clara County," *The Mercury News*, June 7, 2016.
http://www.mercurynews.com/2016/06/07/pioneering-spy-tech-law-adopted-by-santa-clara-county/.

[61] Ibid.

long will we have the information? Who'll have access? How will we know if there's misuse or abuse? I think we ought to know those answers before we spend millions of dollars in public funds."

The ordinance also provides that the Board of Supervisors, "...shall assess whether the benefits to the impacted County departments and the community of the surveillance technology outweigh the costs – including both the financial costs and reasonable concerns about the impact on and safeguards for privacy, civil liberties and civil rights."

"I firmly believe we can both protect the public, and respect the public's privacy and due process rights," Simitian said. "In fact, I believe we're obligated to do both."

The new measure is noteworthy, in part, because it both addresses specific existing technologies (like surveillance cameras, automated license plate readers, and cell-site simulators), but also attempts to be "future-proof," by describing the kinds of surveillance covered.[62]

Bay Area Rapid Transit's (BART's) proposed Surveillance Policy

According to representatives at BART, the BART Board of Directors will be considering a proposal that would require board approval of any surveillance tools used by BART police or other BART entity.

The ACLU of Northern California, the Oakland Privacy Working Group, and the Electronic Frontier Foundation (EFF) all have indicated support for such the surveillance policy, which has been presented to BART's technology committee in December 2016. A senior attorney at EFF stated: "BART could take a big step forward toward accountability and transparency by passing the ordinance, which will ensure public and collective board oversight of whether to acquire dangerous and invasive spying tools."[63]

Proposed California State Senate Bill

SB 21 (2017), the Police Surveillance Transparency bill[64] sponsored by Senator Jerry Hill, D–San Mateo, would extend existing privacy standards for ALPRs and cell-intercept devices to all surveillance technology used by law enforcement agencies.

"SB 21 ensures that the same privacy protocols and standards that currently apply to license plate readers and cell site simulators apply to all other surveillance technology, including those developed in the future," Senator Hill said.[65]

This bill was passed by the California State Senate on May 31, 2017 and was then sent to the California Assembly.[66]

---

62 Press Release: "Joe Simitian: Cutting-edge surveillance ordinance approved for Santa Clara County," accessed May 6, 2017. https://www.sccgov.org/sites/d5/newsmedia/press-releases/Pages/SurveillanceOrdinance.aspx.

63 Joe Kukura "BART Considers Measure to Limit Surveillance," *SF Weekly*, January 26, 2017. http://www.sfweekly.com/news/bart-considers-measure-to-limit-surveillance/.

64 Text of bill is available at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB21.

65 "New Legislation," Senator Jerry Hill, accessed April 3, 2017. https://lcmspubcontact.lc.ca.gov/PublicLCMS/imgs/SD13/2017/jan/Hill_eNews_010317_Full.htm#article1.

66 "CA SB21|2017-2018|Regular Session," Legiscan, accessed June 1, 2017. https://legiscan.com/CA/bill/SB21/2017ncric.

FINDINGS

F1. The County of Santa Clara passed an ordinance in 2016 requiring agencies to adopt policies related to any surveillance technology before such technology is acquired or activated. The ordinance also requires agencies to issue annual reports explaining how the technologies are used and what they discovered.

F2. The County and cities in San Mateo County have not enacted any ordinances governing their acquisition and use of surveillance technology, or the accessibility, management, or retention of the information acquired.

F3. The County and cities in San Mateo County do inform residents about the use of some surveillance tools (Automated License Plate Readers and Body Worn Cameras) at public forums and city council meetings:

- City or Town Council meeting or staff reports posted on website: Atherton, Burlingame, Daly City, East Palo Alto, Hillsborough, Menlo Park, Pacifica, Redwood City, San Bruno, San Carlos, San Mateo, South San Francisco
- Public meeting or Town Halls: East Palo Alto, Hillsborough, Menlo Park, Redwood City, San Carlos, Sheriff's Office
- The City of Menlo Park mentioned also having used social media for this purpose.

F4. With the exception of Burlingame, which borrowed ALPR technology, the cities and the San Mateo County Sheriff's Office have complied with the law requiring ALPR users to "conspicuously" post a link to the ALPR usage and privacy policy on their websites.

F5. With the exception of the City of San Mateo, the generic ALPR policies posted by cities and the Sheriff's Office do not provide specific information that helpful to residents.

RECOMMENDATIONS

R1. In addition to providing a conspicuous link to usage and privacy policies on operator websites (as required by law for ALPRs), all law enforcement agencies in the County should create an easily accessible and simply written information webpage by December 31, 2017, which lists the types of surveillance tools (such as ALPRs) and investigative tools (such as ShotSpotter and body worn cameras) utilized by the agency. At a minimum, such a webpage shall include these details about each tool:

- What is the use and purpose of the technology, such as assisting in ongoing criminal investigations, locating missing children, or locating stolen vehicles
- Who is authorized to collect or access the data collected
- How the system is monitored to ensure that the data are secure
- Who owns the surveillance technology
- What measures were taken to ensure the accuracy of the data
- How long the data will be retained

R2. All law enforcement agencies in the County shall increase the number and types of opportunities for community members to voice support for or opposition to any proposed addition of new surveillance technologies including, but not limited to:

- Surveying residents to better understand their concerns about law enforcement's use of surveillance tools and address those concerns in public meetings, Town Halls, Neighborhood Watch sessions and other local gatherings.
- Using social media platforms such as Nextdoor© to keep residents engaged and informed about surveillance technologies and its uses in your community.

R3. Staff shall bring to the city or town council (in the case of a police department or police bureau) or the Board of Supervisors (in the case of the Sheriff's Office) a policy or ordinance for consideration at a public meeting by December 31, 2017. Such ordinances or policies should require, at a minimum:

- Plans to acquire new surveillance technology be announced at public meetings and other forums to ensure that the community is aware and engaged when new technology is under consideration.
- Any "use policies" related to surveillance technology be readily available and easy to access on the city or County websites.
- Oversight and accountability be supported by posting periodic reports on the effectiveness of the surveillance tools used in the community.

REQUEST FOR RESPONSES

Pursuant to Penal code section 933.05, the Grand Jury requests responses to **Recommendations 1-3** from the following:

- San Mateo County Board of Supervisors
- San Mateo County Sheriff's Office
- Broadmoor Police Protection District
- Atherton Town Council
- Belmont City Council
- Brisbane City Council
- Burlingame City Council
- Colma City Council
- Daly City City Council
- East Palo Alto City Council
- Foster City City Council
- Half Moon Bay City Council

- Hillsborough Town Council
- Menlo Park City Council
- Millbrae City Council
- Pacifica City Council
- Portola Valley Town Council
- Redwood City City Council
- San Bruno City Council
- San Carlos City Council
- San Mateo City Council
- South San Francisco City Council
- Woodside Town Council

The governing bodies indicated above should be aware that the comment or response of the governing body must be conducted subject to the notice, agenda and open meeting requirements of the Brown Act.

BIBLIOGRAPHY

ACLU of Northern California *Making Smart Decisions about Surveillance: A Guide for community Transparency, Accountability and Oversight, April 2016.* https://www.aclunc.org/docs/20160325-making_smart_decisions_about_surveillance.pdf.

Bartley, Kaitlyn. "Dashboard cameras rolled out before policy." *Half Moon Bay Review*, February 23, 2017. http://www.hmbreview.com/news/dashboard-cameras-rolled-out-before-policy/article_b2329fe6-f9f8-11e6-9172-3fb3fe109222.html.

BondGraham, Darwin. "Oakland Privacy Commission Approves Surveillance Transparency Oversight Law." *East Bay Express,* January 6, 2017. http://www.eastbayexpress.com/SevenDays/archives/2017/01/06/oakland-privacy-commission-approves-surveillance-transparency-and-oversight-law.

Electronic Frontier Foundation. "California Automatic License Plate Reader Policies," Electronic Frontier Foundation. Accessed March 30, 2017. https://www.eff.org/pages/california-automated-license-plate-reader-policies.

Electronic Frontier Foundation. "Street-Level Surveillance: Automated License Plate Readers." Accessed May 23, 2017. https://www.eff.org/sls/tech/automated-license-plate-readers.

Electronic Frontier Foundation. "Street-Level Surveillance: Cell-site Simulators." Accessed May 23, 2017. https://www.eff.org/sls/tech/cell-site-simulators.

Goins, Cole. "What Oakland, California, residents think about police surveillance." *Reveal from the Center for Investigative Reporting*, August 18, 2015. https://www.revealnews.org/article/what-oakland-california-residents-think-about-police-surveillance/.

Hofer, Brian. "How the fight to stop Oakland's Domain Awareness Center Laid the Groundwork for the Oakland Privacy Commission." *ACLU of Northern California* (blog), Sept. 21, 2016. https://www.aclunc.org/blog/how-fight-stop-oaklands-domain-awareness-center-laid-groundwork-oakland-privacy-commission.

Kukura, Joe. "BART Considers Measure to Limit Surveillance." *SF Weekly*, January 26, 2017. http://www.sfweekly.com/news/bart-considers-measure-to-limit-surveillance/.

Kurhi, Eric. "Pioneering spy-tech law adopted by Santa Clara County," *The Mercury News*, June 7, 2016. http://www.mercurynews.com/2016/06/07/pioneering-spy-tech-law-adopted-by-santa-clara-county/.

Kendall, Marisa. "Surveillance in Silicon Valley is hard to avoid." *The Mercury News*, February 9, 2017. http://www.mercurynews.com/2017/02/09/surveillance-in-silicon-valley-whos-watching-you/.

LaCambra, Stephanie. "Congressional Oversight Committee Wants to Rein in Police Abuse of Cell-Site Simulators," *Electronic Frontier Foundation DeepLinks* (blog) https://www.eff.org/deeplinks/2017/02/bipartisan-congressional-oversight-committee-wants-probable-cause-warrants-0.

Maass, David. "Success in Sacramento: Four New Laws. One Veto—All Victories for Privacy and Transparency." Accessed June 2, 2017. https://www.eff.org/deeplinks/2015/10/success-sacramento-four-new-laws-one-veto-all-victories-privacy-and-transparency.

McLeod, Saul. "Maslow's Hierarchy of Needs." Simply Psychology. Accessed May 23,2017. https://www.simplypsychology.org/maslow.html.

NCRIC Northern California Regional Intelligence Center. "How the NCRIC was Established." Accessed April 19, 2017. https://ncric.org/default.aspx?MenuItemID=122&MenuGroup=NCRIC+Public+Home&AspxAutoDetectCookieSupport=1.

NCRIC Northern California Regional Intelligence Center. "Frequently Asked Questions." Accessed May 18, 2017. https://ncric.org/html/ALPR-FAQ-Feb-2015.pdf.

Police Executive Research Forum. "How Are Innovations in Technology Transforming Policing." http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.

Seipel, Tracy and Eric Kurhi. "California Digital Privacy Laws Boosted Protecting Consumers from Big Brother, Big Business," *San Jose Mercury News*, October 9. 2015. http://www.mercurynews.com/2015/10/09/california-digital-privacy-laws-boosted-protecting-consumers-from-big-brother-big-business/.

San Mateo County Grand Jury 2015-16. *Body Cameras—The Reel Issue*. https://www.sanmateocourt.org/documents/grand_jury/2015/body_camera.pdf.

San Mateo County Grand Jury 2016-2017. *Summary of Responses to the 2015-2016 San Mateo County Civil Grand Jury Final Reports, (Second Summary)*. As of June 6, 2017, this report is not yet available online.

Tulchin Research."California Statewide Survey Finds Voters Concerned about Privacy and Want to See Reforms Made to Surveillance Technology Use by Law Enforcement." August 21, 2015. http://www.aclunc.org/docs/20150821-aclu_surveillance_privacy_polling.pdf.

U.S. Department of Homeland Security. "State and Major Urban Area Fusion Centers." Accessed March 30, 2017. https://www.dhs.gov/state-and-major-urban-area-fusion-centers.

Weigel, Samantha. "Who's watching who?: License plate readers used throughout San Mateo County." *The Daily Journal*, April 8, 2015. http://www.smdailyjournal.com/articles/lnews/2015-04-08/whos-watching-who-license-plate-readers-used-throughout-san-mateo-county/1776425141346.html.

Winston, Ali. "License plate readers tracking cars." *SFGate*, June 25, 2013. http://www.sfgate.com/bayarea/article/License-plate-readers-tracking-cars-4622476.php.

APPENDIX A

NCRIC Automated License Plate Reader Policy

NCRIC MISSION

The Northern California Regional Intelligence Center (NCRIC) is a multi-jurisdiction public safety program created to assist local, state, federal, and tribal public safety agencies and critical infrastructure locations with the collection, analysis, and dissemination of criminal threat information. It is the mission of the NCRIC to protect the citizens within its area of responsibility from the threat of narcotics trafficking, organized crime, as well as international, domestic, and street terrorism-related activities through information sharing and technical operations support to public safety personnel.

AUTOMATED LICENSE PLATE READER (ALPR) TECHNOLOGIES

To support authorized law enforcement and public safety purposes of local, state, federal, and tribal public safety agencies, the NCRIC utilizes Automated License Plate Reader (ALPR) technology, and supporting software, to gather and analyze ALPR data to enable the rapid identification and location of vehicles of legitimate interest to law enforcement. ALPR units are attached to law enforcement vehicles or deployed at fixed locations, where they collect license plate information from vehicles on public roadways and public property. In one common use of ALPR technology, license plate encounters are compared against law enforcement "hotlists" – lists of vehicles associated with active investigations, for example, related to Amber Alerts or other missing children, stolen vehicles, or stolen license plates. The information is also retained for a fixed retention period, though it is only reaccessible by law enforcement given a legitimate law enforcement purpose as listed below.

PURPOSE

This NCRIC Automated License Plate Reader Policy (ALPR Policy) defines a minimum set of binding guidelines to govern the use of Automated License Plate Reader Data (ALPR Data), in order to enable the collection and use of such data in a manner consistent with respect for individuals' privacy and civil liberties.
The NCRIC also completed a NCRIC ALPR Privacy Impact Assessment (PIA) to address in further detail common privacy and civil liberties concerns regarding Automated License Plate Reader technology. The current version of this document is available on the NCRIC web site at www.ncric.org.

AUTHORIZED PURPOSES, COLLECTION, AND USE OF ALPR DATA

To support the mission of the NCRIC, Law enforcement personnel with a need and right to know will utilize ALPR technology to:

- Locate stolen, wanted, and subject of investigation vehicles;
- Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement;
- Locate witnesses and victims of violent crime;
- Locate missing children and elderly individuals, including responding to Amber and Silver Alerts;
- Support local, state, federal, and tribal public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes;
- Protect participants at special events; and
- Protect critical infrastructure sites.

RESTRICTIONS ON COLLECTION OF ALPR DATA AND USE OF ALPR SYSTEMS

NCRIC ALPR units may be used to collect data that is within public view, but may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution.

ALPR operators may not contact occupants of stolen, wanted, or subject-of-investigation vehicles unless the ALPR operators are sworn law enforcement officers. ALPR operators must rely on their parent agency rules and regulations regarding equipment, protection, self-identification, and use of force when stopping vehicles or making contact.

ALPR operators must recognize that the data collected from the ALPR device, and the content of referenced hotlists, consists of data that may or may not be accurate, despite ongoing efforts to maximize the currency and accuracy of such data. To the greatest extent possible, vehicle and subject information will be verified from separate Law enforcement information sources to confirm the vehicle or subject's identity and justification for contact. Users of ALPR Data must, to the fullest extent possible, visually confirm the plate characters generated by the ALPR readers correspond with the digital image of the license plate in question.

All users of NCRIC ALPR equipment or accessing NCRIC ALPR Data are required to acknowledge that they have read and understood the NCRIC ALPR Policy prior to use of the ALPR System.

In no case shall the NCRIC ALPR system be used for any purpose other than a legitimate law enforcement or public safety purpose.

TRAINING

Only persons trained in the use of the NCRIC ALPR system, including its privacy and civil liberties protections, shall be allowed access to NCRIC ALPR Data. Training shall consist of:

- Legal authorities, developments, and issues involving the use of ALPR Data and technology
- Current NCRIC Policy regarding appropriate use of NCRIC ALPR systems;
- Evolution of ALPR and related technologies, including new capabilities and associated risks;
- Technical, physical, administrative, and procedural measures to protect the security of ALPR Data against unauthorized access or use; and
- Practical exercises in the use of the NCRIC ALPR system

Training shall be updated as technological, legal, and other changes that affect the use of the NCRIC ALPR system occur.

AUDIT

Access to, and use of, ALPR Data is logged for audit purposes. Audit reports will be structured in a format that is understandable and useful and will contain, at a minimum:

- The name of the law enforcement user;
- The name of the agency employing the user;
- The date and time of access;
- The activities executed, including any license plates searched for;
- The supplied authorized law enforcement or public safety justification for access; and
- A case number associated with the investigative effort generating the ALPR data query.

Audit reports will be provided periodically and on request to supervisory personnel at t the NCRIC and partner agencies.

In addition, no less frequently than every 12 months, the NCRIC will audit a sampling of ALPR system utilization from the prior 12 month period to verify proper use in accordance with the above authorized

uses. Any discovered intentional misconduct will lead to further investigation, termination of system access, and notification of the user's parent agency for appropriate recourse. In addition, the auditing data will be used to identify systemic issues, inadvertent misuse, and requirements for policy changes, training enhancements, or additional oversight mechanisms.

These ALPR audits shall be conducted by a senior NCRIC official other than the person assigned to manage the NCRIC ALPR function. Audit results shall then be reported to the Director of the NCRIC.

DATA QUALITY AND ACCURACY

The NCRIC will take reasonable measures to ensure the accuracy of ALPR Data collected by NCRIC ALPR units and partner agency ALPR systems. Errors discovered in ALPR Data collected by NCRIC ALPR units are marked, corrected, or deleted in accordance with the type and severity of the error in question. Errors discovered in ALPR Data collected from partner agencies' ALPR systems are communicated back to the controlling agency to be addressed as deemed appropriate by that agency or in accordance with the agency's own ALPR data policies.

As the downstream custodian of "hotlists", the NCRIC will provide the most recent versions of these lists available and ensure the lists are refreshed from state or federal sources on a daily basis.

The NCRIC acknowledges that, in rare instances ALPR units may inadvertently capture information contrary to the collection guidelines set forth in this policy. Such records will be purged upon identification. Any discovered notable increase in frequency of these incidents from specific ALPR units or agencies will be followed up with for equipment repairs, camera realignment, or personnel training as necessary.

PHYSICAL AND ELECTRONIC SECURITY OF ALPR DATA:

Data collected by ALPR systems is stored in a secured law enforcement facility with multiple layers of physical security and 24/7 security protections. Physical access is limited to law enforcement staff in good standing who have completed background investigations and possess an active security clearance at the "SECRET" or higher level.

NCRIC will utilize strong multi-factor authentication, encrypted communications, firewalls, and other reasonable physical, technological, administrative, procedural, and personnel security measures to mitigate the risks of unauthorized access to the system.

RETENTION OF ALPR DATA:

ALPR Data collected by NCRIC ALPR units or shared from partner agencies' ALPR units shall not be retained longer than 12 months, or the length of time required by the partner agency who is custodian of the record – whichever is shorter. Once the retention period has expired, the record will be purged entirely from all active and backup systems unless a reasonable suspicion has been established that the vehicle identified by the ALPR read is connected to criminal activities.

ALPR records matching an entry in a current law enforcement hotlist will trigger an immediate notification to the officer operating the ALPR unit, the active dispatch officer at the agency owning the ALPR unit, the NCRIC, and the custodial agency of the hotlist. Such notifications are also subject to a maximum retention of 12 months.

ALPR Data obtained with license plate information not appearing on hotlists, and with no immediate reasonable connection to criminal activity, will be retained in secure systems so as to only be made accessible to authorized personnel for a maximum period of twelve months, then purged entirely from all systems. If during the specified retention period there is information which supports a legitimate law enforcement purpose (see above section enumerating AUTHORIZED PURPOSES, COLLECTION, AND USE OF ALPR DATA) as to a license plate or partial license plate which was recorded and is retained in these systems, then limited access will be permitted for predicate-based querying for potential matches

against the parameters specific to the legitimate law enforcement purpose. Such events shall be recorded in an access log showing date, time, name of person seeking access, agency of employment, reason for access, and tracking identifiers such as an agency case number.

NCRIC Automated License Plate Reader Policy 5 ALPR records of vehicles having been identified and linked to criminal investigation will be entered into the relevant NCRIC database(s) and retained for a period of no more than five years. If during the fiveyear period NCRIC personnel become aware that the vehicle license plate information is no longer associated with a criminal investigation, it will be purged from the NCRIC's databases.

CUSTODIAN OF RECORDS AND RECORDS REQUESTS

Each agency operating ALPR technology retains control and ownership as the official custodian of its records, and must independently verify all external information obtained via NCRIC Information Systems. To the extent permitted by law, requests for information under the California Public Records Act or Freedom of Information Act or similar applicable laws will be directed back to the owner of the requested data.

SYSTEM MANAGEMENT AND ACCOUNTABILITY

The NCRIC shall assign a senior officer who will have responsibility, and be accountable, for managing the ALPR Data collected and ensuring that the privacy and civil liberties protection and other provisions of this ALPR Policy are carried out. This individual shall also be responsible for managing a process for maintaining the most current and accurate hotlists available from NCRIC law enforcement sources. This individual shall also have the responsibility for the security of the hotlist information and any ALPR Data which is maintained by the NCRIC. It remains, however, the personal responsibility of all officers with access to ALPR Data to take reasonable measures to protect the privacy and civil liberties of individuals, as well as the security and confidentiality of ALPR Data.

COMMERCIALLY CREATED ALPR DATA

Except as explicitly authorized below with regard to critical infrastructure, the NCRIC will not share NCRIC or partner agency ALPR Data with commercial or other private entities or individuals.

DISSEMINATION

The NCRIC may disseminate ALPR data to any governmental entity with an authorized law enforcement or public safety purpose for access to such data. The NCRIC assumes no responsibility or liability for the acts or omissions of other agencies in making use of the ALPR data properly disseminated. Though the NCRIC will make every reasonable effort to ensure the quality of shared ALPR Data and hotlists, it cannot make absolute guarantees of the accuracy of information provided.

ALPR Information may be disseminated to owners and operators of critical infrastructure in circumstances where such infrastructure is reasonably believed to be the target of surveillance for the purpose of a terrorist attack or other criminal activity. In these situations, the NCRIC also will make notification to appropriate local, state, and federal law enforcement agencies.

Information collected by the ALPR system shall not be disseminated to private parties, other than critical infrastructure owners or operators, as limited above, unless authorized, in writing, by the Director of the NCRIC or his designee. ALPR information shall not be disseminated for personal gain or for any other non-law enforcement purposes.

POLICY REVISIONS

NCRIC ALPR Policies will be reviewed, and updated as necessary, no less frequently than every 12 months, or more frequently based on changes in data sources, technology, data use and/or sharing agreements, and other relevant considerations.

The most current version of the ALPR Policy may be obtained from the NCRIC website at http://www.ncric.org/

APPENDIX B

TULCHIN RESEARCH
Polling & Strategic Consulting

August 21, 2015

To: Interested Parties

From: Ben Tulchin, Corey O'Neil and Kiel Brunner; Tulchin Research

Re: **California Statewide Survey Finds Voters Concerned about Privacy and Want to See Reforms Made to Surveillance Technology Use by Law Enforcement**

Tulchin Research recently conducted a California statewide survey on behalf of the ACLU of California Center for Advocacy & Policy to assess how likely voters think and feel about criminal justice and law enforcement, including how police use surveillance technology to track internet, text, e-mail and other digital activity via hand held devices and computers. With the issue of privacy and surveillance in the news in recent years, this research aims to gauge voter sentiments toward these issues in California specifically and help inform local elected officials in Sacramento about the public's desire to reform how law enforcement tracks and observes the online actions of California residents.

We provide below a summary of the key findings from the survey.

Police Access to Digital Surveillance

Voters in California broadly support a myriad of reforms to ensure their online communications and activities are not tracked by law enforcement without a warrant. When it comes to accessing e-mail and internet activity, more than four out of five voters (82 percent) support requiring a warrant prior to authorities gaining access. Similarly, nearly four out of five voters (79 percent) support this requirement for allowing cell phone access and 77 percent for text messaging records.

The table below shows the statewide results among likely voters.

Support for Requiring Police to Get a Warrant to Monitor Online Activity and Communications

Here are some suggested proposals to improve transparency and accountability for police use of surveillance technology. Please indicate whether you support or oppose each proposal.

	Support	Oppose	Und.	Supp – Opp
Require police officers to get a warrant before they can access your ***Internet use and what you do online.***	82%	12%	6%	+71
Require police officers to get a warrant before they ***can access your e-mail.***	82%	10%	8%	+72
Require police officers to get a warrant before they ***track your cell phone and what you do on it.***	79%	12%	10%	+67
Require police officers to get a warrant before they ***can access your text messages.***	77%	14%	9%	+63

182 Second Street, Suite 400 • San Francisco, CA 94105 • (415) 874-7441

In looking specifically at the high levels of support for requiring law enforcement to obtain a warrant prior to conducting surveillance of online activity (82 percent support), this proposal garners overwhelming backing from across majorities of every key demographic group in the state including:

- Both women (83 percent support) and men (81 percent) show strong support for this reform;
- All ethnic groups including Latinos (93 percent), African Americans (88 percent), Asians (87 percent) and Caucasians (78 percent);
- Bridging the partisan divide, Democratic (87 percent), Republican (74 percent) and independent (83 percent) voters all broadly support requiring a warrant in this context; and
- Voters of all ages agree that police should get a warrant prior to tracking online use with voters ages 18 to 29 most in favor (90 percent), followed by voters ages 30 to 49 (83 percent), voters ages 50 to 64 (82 percent) and voters ages 65 and older (79 percent).

Support for Requiring Police to Get a Warrant to Access Internet Use (By Demographic Group)

Here are some suggested proposals to improve transparency and accountability for police use of surveillance technology. Please indicate whether you support or oppose each proposal.

Require police officers to get a warrant before they can access your internet use and what you do online

	Support	Oppose	Supp-Opp
All California Voters	**82%**	**12%**	**+71**
Gender			
Women	83%	11%	+72
Men	81%	13%	+69
Ethnicity			
Blacks	88%	5%	+81
Latinos	93%	6%	+86
Asians	87%	4%	+83
Whites	78%	15%	+62
Party			
Democrats	87%	7%	+80
Republicans	74%	18%	+56
Independents	83%	13%	+70
Age			
18-29	90%	9%	+81
30-39	83%	12%	+71
40-49	83%	10%	+73
50-64	82%	11%	+70
65+	79%	14%	+65

Voters in the state also carry strong sentiments about requiring law enforcement to obtain a warrant before tracking cell phone usage and activity (79 percent support). Similar to online activity above, every demographic group shares this strong support for protecting their privacy on their mobile devices:

- Both men (82 percent) and women (75 percent) offer strong support for requiring a warrant to track cell phones and what individuals do on their phones;
- Cell phone privacy strikes a chord most notably among Asian (95 percent) and African American voters (93 percent), while there is also support from over three-quarters of white and Latino (77 percent) voters;
- Voters of all parties support requiring warrants for police to access cell phone data and activity as Democratic (81 percent), Republican (74 percent) and independent (79 percent) voters all approve of this measure; and
- Among various age groups, support for cell phone privacy is strongest among voters ages 50 to 64 (82 percent) and is followed closely by voters ages 65 and older (79 percent), ages 40 to 49 (78 percent), and voters age 18-39 (74 support).

Cell Phone Use Requirement Proposal (By Demographic Group)

Here are some suggested proposals to improve transparency and accountability for police use of surveillance technology. Please indicate whether you support or oppose each proposal.

Require police officers to get a warrant before they track your cell phone and what you do on it.

	Support	Oppose	Supp-Opp
All California Voters	79%	12%	+67
Gender			
Women	75%	11%	+64
Men	82%	13%	+70
Ethnicity			
Blacks	93%	4%	+88
Latinos	77%	10%	+67
Asians	95%	0%	+95
Whites	77%	13%	+64
Party			
Democrats	81%	7%	+74
Republicans	74%	16%	+58
Independents	79%	15%	+64
Age			
18-29	74%	14%	+62
30-39	74%	12%	+63
40-49	78%	11%	+67
50-64	82%	12%	+70
65+	79%	11%	+68

In addition to these previously mentioned technology-specific surveillance measures, voters also would like to see reforms implemented at the state and local level of surveillance practices by law enforcement in order to provide more oversight, accountability and limits to this law enforcement tactic. Among them, two-thirds of voters would like to see local elected officials like City Councilmembers or County Supervisors approve new surveillance technologies before they can be used (67 percent support). Similarly, voters want to see policies set that limit surveillance use both locally (65 percent) and statewide (64 percent). Voters also want to see steps taken to require public reporting from law enforcement agencies regarding the frequency of use of surveillance technologies (62 percent) as well as providing public notification before purchasing any new surveillance technologies (58 percent).

Support for Local and State Surveillance Reforms

Here are some suggested proposals to improve transparency and accountability for police use of surveillance technology. Please indicate whether you support or oppose each proposal.

	Support	Oppose	Don't Know	Supp – Opp
Require the local City Council or Board of Supervisors to vote to approve new surveillance technology before it is used by local police.	67%	19%	14%	+48
Develop and enforce local policies to set limits on surveillance technology used by police.	65%	18%	17%	+47
Develop and enforce statewide policies to set limits on surveillance technology used by police.	64%	18%	18%	+47
Require law enforcement agencies to publicly report how often they are using surveillance.	62%	24%	13%	+47
Provide public notification prior to local police buying new technology for surveillance.	58%	23%	19%	+36

Conclusion

These findings show wide support throughout California for limiting how law enforcement uses surveillance technologies on the public. From internet and e-mail surveillance to cell phone and text messaging activities, voters from across a spectrum of demographic and partisan groups show strong support for reforming how law enforcement tracks our activities through technology by requiring the police to get a warrant before collecting this information. More broadly, voters want more accountability, oversight and limits placed on police surveillance tactics.

Survey Methodology: *Tulchin Research conducted a statewide survey in California among 900 likely November 2016 voters, including a statewide base sample of 800 voters and an oversample of 100 African American voters. The oversample of African American voters provides increased statistical confidence for that specific demographic, especially in looking at key sub-groups. Interviews were conducted online from July 10-14, 2015. The margin of error for the statewide base sample is +/- 3.46 percent.*

APPENDIX C

This table shows the verbatim responses to this question from the Grand Jury's survey of police departments and the Sheriff's Office: "Before purchasing the technology, did you inform residents of your intention to acquire surveillance tools?"

City	How Cities Responded
Atherton	The projects and expenses were approved by the Town Council and divulged as part of the public agenda in staff reports.
Belmont	*Belmont did respond "Yes" to the question but did not provide details.*
Broadmoor	N/A *(no surveillance technology in use).*
Brisbane	*Law enforcement did not reach out to the community*
Burlingame	Body Worn Cameras we responded to the Grand Jury's recommendation to implement and went before our City Council for approval. GPS we did not notify our community Police Department Cameras we did not notify our community
Colma	N/A *(no surveillance technology in use).* Note: The Police Department will reach out to residents at council meetings and social media if the Department does plan to acquire surveillance technology.
Daly City	Staff report to City Council for approval
East Palo Alto	ShotSpotter: This was installed during Chief Ronald Davis tenure and I believe there was involvement with community and the matter was approved by the City Council. Additionally, each year that I renew the contract, it goes before the City Council and the community has the opportunity to comment on the use of the system.
Foster City	*Law enforcement did not reach out to the community*
Hillsborough	The ALPR mobile unit purchase was introduced over the course of several council meetings and approved by City Council. We also hosted a number of community forums on the topic of crime prevention and discussed the ALPR technology prior to and after it was approved. Additionally, we regularly update our council with details and statistics from our ALPR program.

City	How Cities Responded
Menlo Park	City council meetings, social media, community meetings
Millbrae	N/A *(no surveillance technology in use)*
Pacifica	Regarding the implementation of patrol vehicle cameras in the mid 1990's, it is unknown what methods were used to inform residents. The police department's body camera implementation plan was announced at a City Council meeting. When body cameras are deployed, the department plans to announce this vial social media and press release.
Redwood City	We did community outreach and held a community meeting regarding the placing of surveillance cameras on a pedestrian footbridge. Redwood City Police Department began using the ALPR technology in 2012. On October 6, 2015, Governor Edmund G. Brown Jr. signed SB 34, which added provisions to the California Civil Code regarding the use of ALPR systems, including requiring government agencies using ALPRs to maintain reasonable security procedures and practices, to implement a privacy policy, to keep records of access to records created through use of ALPR system, and to prevent unauthorized access to the system. In addition, the agency must disclose any security breaches and cannot sell, share, or transfer ALPR information, except to another public agency and only as permitted by law. Under Section 1798.90.55 (a), the new law requires: A public agency that operates or intends to operate an ALPR system shall provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing the program. The Police Department has updated its Policy Manual to comply with the new provisions of the law. The updated policy regarding Automated License Plate Readers has been posted to the City Website as required by California Civil Code Section 1798.90.51 (b)(1). Because the department began using ALPR technology prior to the passage of SB 34, compliance with the requirement that an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before

City	How Cities Responded
	implementing the program was not possible. The Department is in compliance with SB34 and is now providing an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before implementing new ALPR technology.
San Bruno	A staff report regarding the ALPR was made available on the city's web page. The project was also presented in a televised public forum at a city council meeting.
San Carlos	The decision to deploy ALPR technology was made by the City Council; not by the Police Bureau. An open, "noticed" public meeting was held to discuss the item and take public comment on the issue. At the conclusion of that very public process, the city Council voted and directed the Police Bureau to deploy the ALPRs We also discussed the issue during Police Town Hall Meetings and Neighborhood Watch events.
San Mateo (city)	Depends—ALPRs are required by law to be noticed to our city council and we posted the privacy policy on our internet
San Mateo County Sheriff	Open, noticed public meetings were held to discuss the items and take public comment on the issue. The meetings were held to help educate and inform the community. During the community meetings, we provided facts and also discussed the benefits during Town Hall Meetings and Neighborhood Watch events.
South San Francisco	Our intention to acquire body cameras was addressed at a public City Council meeting. Once the body cameras are implemented, we will make a public announcement by means of a press release and social media

Issued: July 12, 2017

Town of Atherton
Office of the Mayor
91 Ashfield Road
Atherton, California 94027
Phone: (650) 752-0500
Fax: (650) 614-1212

September 21, 2017

Hon. Leland Davis, III
Judge of the Superior Court
c/o Charlene Kresevich
Hall of Justice
400 County Center; 2nd Floor
Redwood City, CA 94063-1655

RESPONSE TO GRAND JURY REPORT: "A DELICATE BALANCE: PRIVACY VS. PROTECTION."

Honorable Judge Davis –

Thank you for the opportunity to review and comment on the above referenced Grand Jury Report filed on July 12, 2017. The Town of Atherton's response to both the findings and recommendations are listed below.

Response to Grand Jury Findings:

F1. The County of Santa Clara passed an ordinance in 2016 requiring agencies to adopt policies related to any surveillance technology before such technology is acquired or activated. The ordinance also requires agencies to issue annual reports explaining how the technologies are used and what they discovered.
Response to F1: The Town agrees with this finding, relying on the Grand Jury's representations in their report.

F2. The County and cities in San Mateo County have not enacted any ordinances governing their acquisition and use of surveillance technology, or the accessibility, management, or retention of the information acquired.
Response to F2: The Town agrees with this finding, relying on the Grand Jury's representations in their report.

F3. The County and cities in San Mateo County do inform residents about the use of some surveillance tools (Automated License Plate Readers and Body Worn Cameras) at public forums and city council meetings:

- **City or Town Council meeting or staff reports posted on website: Atherton, Burlingame, Daly City, East Palo Alto, Hillsborough, Menlo Park, Pacifica, Redwood City, San Bruno, San Carlos, San Mateo, South San Francisco**
- **Public meeting or Town Halls: East Palo Alto, Hillsborough, Menlo Park, Redwood City, San Carlos, Millbrae, Portola Valley, Ladera, and Emerald Hills.**
- **The City of Menlo Park mentioned also having used social media for this purpose**

Response to F3: The Town agrees with this finding, relying on the Grand Jury's representations in their report.

F4. With the exception of the Town of Atherton and the City of Burlingame, which borrowed ALPR technology, the cities and the San Mateo County Sheriff's Office have complied with the law requiring ALPR users to "conspicuously" post a link to the ALPR usage and privacy policy on their websites.

Response to F4: The Town agrees with this finding, relying on the Grand Jury's representations in their report.

F5. With the exception of the City of San Mateo, the generic ALPR policies posted by cities and the Sheriff's Office do not provide specific information that helpful to residents.

Response to F5: The Town of Atherton has yet to post its policy on the Town's website until ALPR has been implemented once the new patrol vehicle is equipped and placed in service. The Town has no independent basis on which to agree or disagree with the Grand Jury's finding as to other jurisdictions' policies.

Response to Grand Jury Recommendations:

R1. In addition to providing a conspicuous link to usage and privacy policies on operator websites (as required by law for ALPRs), all law enforcement agencies in the County should create an easily accessible and simply written information webpage by December 31, 2017, which lists the types of surveillance tools (such as ALPRs) and investigative tools (such as ShotSpotter and body worn cameras) utilized by the agency. At a minimum, such a webpage shall include these details about each tool:

- **What is the use and purpose of the technology, such as assisting in ongoing criminal investigations, locating missing children, or locating stolen vehicles**
- **Who is authorized to collect or access the data collected**
- **How the system is monitored to ensure that the data are secure**
- **Who owns the surveillance technology**
- **What measures were taken to ensure the accuracy of the data**
- **How long the data will be retained**

Response to R1: This recommendation will be implemented in part. San Mateo County Law Enforcement Agencies have already, by law, posted privacy policy information on their websites as related to ALPRs. The Town of Atherton will expand its ALPR privacy and usage policy to include additional electronic equipment where the release of such information does not unnecessarily jeopardize public safety and criminal investigations, and will place that information in a conspicuous location on its website by December 31, 2017.

R2. All law enforcement agencies in the County shall increase the number and types of opportunities for community members to voice support for or opposition to any proposed addition of new surveillance technologies including, but not limited to:

- **Survey residents to better understand their concerns about law enforcement's use of surveillance tools and address those concerns in public meetings, Town Halls, Neighborhood Watch sessions and other local gatherings.**
- **Using social media platforms such as Nextdoor© to keep residents engaged and informed about surveillance technologies and its uses in your community.**

Response to R2: The Town of Atherton will implement this recommendation for tools used in the conduct of basic police business such as Body Worn Cameras and ALPRs. Furthermore, the Town of Atherton recognizes that not all community members utilize internet and social media, and will seek opportunities at public meetings, including neighborhood association meetings, neighborhood watch gatherings, and publicly noticed city meetings to share this information.

This recommendation cannot be fully implemented for certain law enforcement investigative tools and techniques primarily used for complex criminal investigations without jeopardizing the ability to gather evidence for the serious crimes in question. Therefore, the Town will not hold public forums or conduct similar outreach on certain investigative techniques or technology where doing so might compromise critical investigations. Checks and balances already exist through the legal system, including various warrant requirements and Fourth Amendment protections, regarding the use of these techniques. Certain specialized electronic tools are precisely aimed at members of criminal organizations, career criminals, and those under investigation for violent crimes, with minimal to no impact to the law-abiding public. The Town does and will continue to take steps to ensure that the informational privacy of persons who are not suspects or involved in such investigations will be respected.

All agencies in San Mateo County have signed a data and records sharing agreement with the Northern California Regional Intelligence Center (NCRIC) that places data in a secure repository located in a federal facility subject to federal and state statutes and policies addressing access, storage, and disclosure.

R3. Staff shall bring to the city or town council (in the case of a police department or police bureau) or the Board of Supervisors (in the case of the Sheriff's Office) a policy or ordinance for consideration at a public meeting by December 31, 2017. Such ordinances or policies should require, at a minimum:

- **Plans to acquire new surveillance technology be announced at public meetings and other forums to ensure that the community is aware and engaged when new technology is under consideration.**
- **Any "use policies" related to surveillance technology be readily available and easy to access on the city or County websites.**
- **Oversight and accountability be supported by posting periodic reports on the effectiveness of the surveillance tools used in the community.**

Response to R3: Existing law requires that Law enforcement agencies provide information to local governing bodies when acquiring certain new technologies. Law enforcement agencies make policies that govern the use of our basic police surveillance tools and technologies publicly available.

However, this recommendation will not be implemented in full because it creates obstacles that could limit law enforcement's ability to adapt and evolve to criminal activity and could compromise the safety and security of residents. Law enforcement agencies may, under certain circumstances, be unable to wait for regularly scheduled public meetings of their governing bodies while in pursuit of criminals and crimes in progress.

Furthermore, existing protections for both personal information and investigatory activities are adequate to address the Grand Jury's concerns. Existing state law, in the form of Government Code 6254(f), exempts investigative, intelligence, and security records from disclosure under the California Public Records Laws. This exception to disclosure protects the integrity of investigations and the criminal legal process, as well as allowing jurisdictions to withhold certain information regarding individuals acquired as a result of an investigation. It is not absolute, however, and the public retains adequate access to information about police activities to be able to monitor a department's overall approach.

Government Code 6254 (f) recognizes the need for discretion and protects law enforcement agencies from disclosing investigative and tactical information that would compromise an agency's crime fighting capabilities. Existing laws also prohibit the release of information derived from, or related to, the security of the agency's technology systems specifically to ensure those upholding and protecting the public are not compromised.

In addition to the guarantees of the Fourth Amendment, California law specifically protects certain kinds of personal information. For example, under California Penal Code 1546 – 1546.4, known as the Electronic Communications Privacy Act, law enforcement is required to obtain court orders related to electronic communications intercept surveillance under Penal Code 629.50, pen register of trap and trace device under Penal Code 630, and for electronic tracking devices court orders are required under Penal Codes 1524 and 1534.

In sum, the Town remains committed to an open and public process regarding law enforcement techniques wherever it is feasible and will not compromise sensitive investigations into serious criminal activity. In those contexts in which a full public discussion is not possible, the Town nonetheless rigorously adheres to existing legal constraints to ensure that both public safety and personal privacy are protected.

This response to the Grand Jury was considered by the City Council at a public meeting on September 20, 2017. Should you have any questions concerning this response, please contact City Manager George Rodericks at (650) 752-0504.

Respectfully,

Michael Lempres
Mayor