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 ShotSpotter2 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.

---

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.

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 show8 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 survey9 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 Reporting11 and three local artists12 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…”

7 Ibid.
8 For information about Tulchin Research, go to http://www.tulchinresearch.com.
9 See Appendix B.
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

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.”

**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.

---


Legislation


  
  “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.\footnote{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.}


- Secure and protect the collected data from “unauthorized access, destruction, use, modification, or disclosure.”\footnote{Ibid.}
- Adopt a usage and privacy policy that is “consistent with respect for any individual’s privacy and civil liberties.”\footnote{Ibid.}
- 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.\footnote{Ibid.}

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

---

• **SB 34 (2015) Automated License Plate Recognition Systems: Use of Data**

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.

In a 2015 *San Jose Mercury News* article, 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.”

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

- 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.

---

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.
30 California Civil Code, sec. 1798.90.51
DISCUSSION

The 2016-2017 San Mateo County Civil Grand Jury (Grand Jury) surveyed 19 local law enforcement agencies 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, 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. 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).

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

**Implementation Coming This Year‡**

<table>
<thead>
<tr>
<th>City/Jurisdiction</th>
<th>Date Implemented</th>
<th>Policy Available Online?</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Bruno</td>
<td>6/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>South San Francisco</td>
<td>7/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Sheriff</td>
<td>10/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Brisbane</td>
<td>10/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Burlingame</td>
<td>10/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Colma</td>
<td>10/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Pacifica</td>
<td>10/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>San Mateo</td>
<td>10/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Redwood City</td>
<td>12/17‡</td>
<td>Not applicable</td>
</tr>
<tr>
<td>East Palo Alto</td>
<td>Fiscal Year 2017-2018‡</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

**No Plans to Purchase BWCs**

<table>
<thead>
<tr>
<th>City/Jurisdiction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadmoor</td>
</tr>
<tr>
<td>Daly City</td>
</tr>
</tbody>
</table>

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.”

The Grand Jury found as follows:

<table>
<thead>
<tr>
<th>Law Enforcement Agency</th>
<th>ALPR Policy Conspicuously Placed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sheriff</td>
<td>Yes. However, the link to the policy is labeled “ALPR Policy.” County residents may not be familiar with the acronym.</td>
</tr>
<tr>
<td>Burlingame</td>
<td>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.</td>
</tr>
<tr>
<td>Daly City</td>
<td>Yes.</td>
</tr>
<tr>
<td>Hillsborough</td>
<td>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.</td>
</tr>
<tr>
<td>Menlo Park</td>
<td>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.</td>
</tr>
<tr>
<td>San Bruno</td>
<td>Yes.</td>
</tr>
<tr>
<td>San Carlos</td>
<td>No. Policy is not available on the website.</td>
</tr>
<tr>
<td>San Mateo</td>
<td>Yes.</td>
</tr>
<tr>
<td>South San Francisco</td>
<td>Yes.</td>
</tr>
</tbody>
</table>

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).\textsuperscript{36} Congress established the NCRIC in 2007, after the Bay Area was designated a high intensity drug trafficking region.\textsuperscript{37} NCRIC’s reach extends from Monterey County to Del Norte County,\textsuperscript{38} covering 15 counties in California.\textsuperscript{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.”\textsuperscript{40}

Access to the NCRIC\textsuperscript{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”\textsuperscript{42} and a “right to know”\textsuperscript{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.\textsuperscript{44}


\textsuperscript{38} Ibid.


\textsuperscript{42} According to the NCRIC “Frequently Asked Questions,” \textit{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.

\textsuperscript{43} According to the NCRIC “Frequently Asked Questions, \textit{Right to know} “…is established when the requester is acting in an official capacity and has statutory authority to obtain the information being sought.”

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

- 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).
- In one year, NCRIC amassed around 46.5 million images from its partner agencies.

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.”

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. 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.

The NCRIC policy provides the following information regarding “custodians”:

**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...
residents wanting to learn about how ALPRs are used in the city.\textsuperscript{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.

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?”\textsuperscript{53} Respondents listed the types of interactions they used to connect with community members.

\begin{center}
\begin{tabular}{|l|l|}
\hline
City & Response\textsuperscript{i} \\
\hline
Atherton & City or Town Council meetings, staff reports posted on city website \\
Burlingame & \\
Daly City & \\
East Palo Alto & \\
Hillsborough & \\
Menlo Park & \\
Pacifica & \\
Redwood City & \\
San Bruno & \\
San Carlos & \\
San Mateo & \\
South San Francisco & \\
\hline
\end{tabular}
\end{center}


\textsuperscript{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.
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. 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.

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. Recently, this commission has proposed a “Surveillance and Community Safety Ordinance,” 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

---

55 Ibid.
56 Ibid.
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

---


\(^{59}\) 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


\(^{61}\) 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 bill64 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

---


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


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


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.


http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20inn%20technology%20transforming%20policing%202012.pdf.


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 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.

**COMMERCIALY 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/
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.

<table>
<thead>
<tr>
<th>Support for Requiring Police to Get a Warrant to Monitor Online Activity and Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proposal</th>
<th>Support</th>
<th>Oppose</th>
<th>Und.</th>
<th>Supp – Opp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require police officers to get a warrant before they can access your internet use and what you do online.</td>
<td>82%</td>
<td>12%</td>
<td>6%</td>
<td>+71</td>
</tr>
<tr>
<td>Require police officers to get a warrant before they can access your e-mail.</td>
<td>82%</td>
<td>10%</td>
<td>8%</td>
<td>+72</td>
</tr>
<tr>
<td>Require police officers to get a warrant before they track your cell phone and what you do on it.</td>
<td>79%</td>
<td>12%</td>
<td>10%</td>
<td>+67</td>
</tr>
<tr>
<td>Require police officers to get a warrant before they can access your text messages.</td>
<td>77%</td>
<td>14%</td>
<td>9%</td>
<td>+63</td>
</tr>
</tbody>
</table>

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.*

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

### 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.

<table>
<thead>
<tr>
<th></th>
<th>Support</th>
<th>Oppose</th>
<th>Supp-Opp</th>
</tr>
</thead>
<tbody>
<tr>
<td>All California Voters</td>
<td>79%</td>
<td>12%</td>
<td>+67</td>
</tr>
</tbody>
</table>

**Gender**

<table>
<thead>
<tr>
<th></th>
<th>Support</th>
<th>Oppose</th>
<th>Supp-Opp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women</td>
<td>75%</td>
<td>11%</td>
<td>+64</td>
</tr>
<tr>
<td>Men</td>
<td>82%</td>
<td>13%</td>
<td>+70</td>
</tr>
</tbody>
</table>

**Ethnicity**

<table>
<thead>
<tr>
<th></th>
<th>Support</th>
<th>Oppose</th>
<th>Supp-Opp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacks</td>
<td>93%</td>
<td>4%</td>
<td>+88</td>
</tr>
<tr>
<td>Latinos</td>
<td>77%</td>
<td>10%</td>
<td>+67</td>
</tr>
<tr>
<td>Asians</td>
<td>95%</td>
<td>0%</td>
<td>+95</td>
</tr>
<tr>
<td>Whites</td>
<td>77%</td>
<td>13%</td>
<td>+64</td>
</tr>
</tbody>
</table>

**Party**

<table>
<thead>
<tr>
<th></th>
<th>Support</th>
<th>Oppose</th>
<th>Supp-Opp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Democrats</td>
<td>81%</td>
<td>7%</td>
<td>+74</td>
</tr>
<tr>
<td>Republicans</td>
<td>74%</td>
<td>16%</td>
<td>+58</td>
</tr>
<tr>
<td>Independents</td>
<td>79%</td>
<td>15%</td>
<td>+64</td>
</tr>
</tbody>
</table>

**Age**

<table>
<thead>
<tr>
<th></th>
<th>Support</th>
<th>Oppose</th>
<th>Supp-Opp</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-29</td>
<td>74%</td>
<td>14%</td>
<td>+62</td>
</tr>
<tr>
<td>30-39</td>
<td>74%</td>
<td>12%</td>
<td>+63</td>
</tr>
<tr>
<td>40-49</td>
<td>78%</td>
<td>11%</td>
<td>+67</td>
</tr>
<tr>
<td>50-64</td>
<td>82%</td>
<td>12%</td>
<td>+70</td>
</tr>
<tr>
<td>65+</td>
<td>79%</td>
<td>11%</td>
<td>+68</td>
</tr>
</tbody>
</table>
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 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

<table>
<thead>
<tr>
<th>Proposal</th>
<th>Support</th>
<th>Oppose</th>
<th>Don’t Know</th>
<th>Supp – Opp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require the local City Council or Board of Supervisors to vote to approve new surveillance technology before it is used by local police.</td>
<td>67%</td>
<td>19%</td>
<td>14%</td>
<td>+48</td>
</tr>
<tr>
<td>Develop and enforce local policies to set limits on surveillance technology used by police.</td>
<td>65%</td>
<td>18%</td>
<td>17%</td>
<td>+47</td>
</tr>
<tr>
<td>Develop and enforce statewide policies to set limits on surveillance technology used by police.</td>
<td>64%</td>
<td>18%</td>
<td>18%</td>
<td>+47</td>
</tr>
<tr>
<td>Require law enforcement agencies to publicly report how often they are using surveillance.</td>
<td>62%</td>
<td>24%</td>
<td>13%</td>
<td>+47</td>
</tr>
<tr>
<td>Provide public notification prior to local police buying new technology for surveillance.</td>
<td>56%</td>
<td>23%</td>
<td>19%</td>
<td>+36</td>
</tr>
</tbody>
</table>

### 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?”

<table>
<thead>
<tr>
<th>City</th>
<th>How Cities Responded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atherton</td>
<td>The projects and expenses were approved by the Town Council and divulged as part of the public agenda in staff reports.</td>
</tr>
<tr>
<td>Belmont</td>
<td>Belmont did respond “Yes” to the question but did not provide details.</td>
</tr>
<tr>
<td>Broadmoor</td>
<td>N/A (no surveillance technology in use).</td>
</tr>
<tr>
<td>Brisbane</td>
<td>Law enforcement did not reach out to the community</td>
</tr>
<tr>
<td>Burlingame</td>
<td>Body Worn Cameras we responded to the Grand Jury’s recommendation to implement and went before our City Council for approval.\n\nGPS we did not notify our community\n\nPolice Department Cameras we did not notify our community</td>
</tr>
<tr>
<td>Colma</td>
<td>N/A (no surveillance technology in use).\n\nNote: The Police Department will reach out to residents at council meetings and social media if the Department does plan to acquire surveillance technology.</td>
</tr>
<tr>
<td>Daly City</td>
<td>Staff report to City Council for approval</td>
</tr>
<tr>
<td>East Palo Alto</td>
<td>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.\n\nAdditionally, 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.</td>
</tr>
<tr>
<td>Foster City</td>
<td>Law enforcement did not reach out to the community</td>
</tr>
<tr>
<td>Hillsborough</td>
<td>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.</td>
</tr>
<tr>
<td>City</td>
<td>How Cities Responded</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Menlo Park</td>
<td>City council meetings, social media, community meetings</td>
</tr>
<tr>
<td>Millbrae</td>
<td>N/A <em>(no surveillance technology in use)</em></td>
</tr>
<tr>
<td>Pacifica</td>
<td>Regarding the implementation of patrol vehicle cameras in the mid 1990’s, it is unknown what methods were used to inform residents.</td>
</tr>
<tr>
<td></td>
<td>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 via social media and press release.</td>
</tr>
<tr>
<td>Redwood City</td>
<td>We did community outreach and held a community meeting regarding the placing of surveillance cameras on a pedestrian footbridge.</td>
</tr>
<tr>
<td></td>
<td>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 the implementation of the program is not required.</td>
</tr>
<tr>
<td>City</td>
<td>How Cities Responded</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>San Bruno</td>
<td>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.</td>
</tr>
<tr>
<td>San Carlos</td>
<td>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.</td>
</tr>
<tr>
<td>San Mateo (city)</td>
<td>Depends—ALPRs are required by law to be noticed to our city council and we posted the privacy policy on our internet.</td>
</tr>
<tr>
<td>San Mateo County Sheriff</td>
<td>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.</td>
</tr>
<tr>
<td>South San Francisco</td>
<td>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.</td>
</tr>
</tbody>
</table>
August 23, 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


Dear Judge Davis:

Thank you for the opportunity to respond to the Grand Jury report entitled “A Delicate Balance: Privacy v. Protection”. The San Mateo County Sheriff’s Office response to both the findings and recommendations are listed below.

Responses 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: The information necessary to either agree or disagree with this finding is not contained within the Sheriff’s Office’s files.

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: The information necessary to either agree or disagree with this finding is not contained within the Sheriff’s Office’s files. However, the Sheriff’s Office has signed a records sharing and data retention agreement for warehousing data with the Northern California Regional Intelligence Center (NCRIC). This agreement ensures that data warehoused within the NCRIC is subject to federal standards and state policies for data retention and sharing.
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: The information necessary to either agree or disagree with this finding is not contained within the Sheriff’s Office’s files. However, the Sheriff’s Office informs residents about the use of surveillance tools at public forums at community and city council meetings.

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.

Response: The information necessary to either agree or disagree with much of this finding is not contained within the Sheriff’s Office’s files. The Sheriff’s Office agrees that it complies 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 is helpful to residents.

Response: The Sheriff’s Office does not agree with this finding and believes that the policy posted on the Sheriff’s Office web page is both specific and helpful to residents. The policy describes authorized purposes, restrictions on collection of data, training, audits, data quality and accuracy, security of data and retention of data.

Responses 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: Portions of this recommendation have already previously been implemented in part and portions will be implemented in part, but portions of the recommendation will not be implemented. The San Mateo County Sheriff’s Office has already posted privacy policy information on its website as to ALPRs. The Sheriff’s Office 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:

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

Response: The Sheriff’s Office will not implement this recommendation because it views its current robust efforts to obtain community input, e.g., as to ALPRs, as having been sufficient and intends to continue its robust efforts if it ever begins using new technologies. The Sheriff’s Office recognizes that not all community members utilize internet and social media, and will continue to seek opportunities at public meetings, including neighborhood association meetings, neighborhood watch gatherings, and publicly noticed meetings to share this information.

This recommendation will also not be implemented for law enforcement investigative tools and techniques primarily used for complex criminal investigative purposes. It is not always appropriate or reasonable for law enforcement agencies to publicly explain and expose certain critical investigative techniques or technology. Checks and balances already exist through the legal system 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.

Public discussion of law enforcement technologies and investigative techniques would be detrimental to ongoing criminal investigations, compromise capabilities to protect communities, and allow individuals involved in criminal activity to more easily avoid detection.

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: Existing law can require 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 when they are public records.

But this recommendation will not otherwise be implemented because it is not warranted or reasonable. The recommendation contains obstacles that would limit law enforcement’s ability to quickly adapt and evolve to criminal activity.

Existing state law protects law enforcement agencies from having to disclose investigative, intelligence and security records under the California Public Records Laws. Government Code 6254 (f) recognizes the need for confidentiality and protects law enforcement agencies from disclosing investigative and tactical information that would compromise crime fighting capabilities. Existing laws also prohibit the release of information derived from, or related to the security of our technology systems specifically to ensure those upholding and protecting the public are not compromised.

It is also of note that, law enforcement agencies are already required to obtain court orders: under California Penal Code 1546 – 1546.4 related to specified electronic communications; under Penal Code 629.50, for wire and other specified electronic communications; and for electronic tracking devices under Penal Codes 1524 and 1534. Further disclosure of advanced investigative technology and techniques would limit law enforcement’s ability to adapt and evolve to criminal activity and would compromise the safety and security of residents of San Mateo County.

Sincerely,

Carlos G. Bolanos
Sheriff
September 21, 2017

Hon. Leland Davis, III
Judge of the Superior Court
c/o Charlene Kesevich
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
September 7, 2017

Honorable Leland Davis, III
Judge of the Superior Court
Hall of Justice
400 County Center, 2nd Floor
Redwood City, CA 94063


Dear Honorable Judge Davis, III:

This letter is in response to the 2016/17 Grand Jury report dated June 29, 2017. The report identifies certain findings and recommendations, and requests that the City Council of Brisbane, respond in writing to those findings no later than September 27, 2017. The Brisbane City Council has approved the below recommendations at their September 7, 2017 meeting.

The San Mateo County 2016-2017 Grand Jury makes the following findings to the City Councils of the cities of San Mateo County:

Findings:

F1. Approximately 130,019 (17.8%) of the residents of San Mateo County self-report that they do not speak English “very well.”

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F2. The 17 law enforcement agencies in San Mateo County provide an impressive 170+ outreach programs.

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F3. The following nine cities’ police departments’ websites provide access to multiple languages. Daly City, East Palo Alto, Hillsborough, Menlo Park, Pacifica, Redwood City, San Bruno, South San Francisco, and the City of San Mateo.
Response: The City of Brisbane partially agrees with this finding. We agree that those cities’ websites listed above provide access to multiple languages. Although the City of Brisbane is not listed, we do indeed provide access to multiple languages via a direct link through Google translate. It was listed on the bottom of the page but may have been overlooked, so we have now moved the link to the top of the page to make it more visibly seen and easily accessible to anyone accessing our website.

F4. The following four cities’ police departments’ websites have no mention of their outreach programs on their websites.

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F5. All seven of the law enforcement agencies listed below consider the language needs of the attendees when planning community outreach events: Daly City Police Department, East Palo Alto Police Department, Redwood City Police Department, San Bruno Police Department, San Mateo Police Department, South San Francisco Police Department, and the San Mateo County Sheriff’s Office.

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F6. All seven of the law enforcement agencies listed below provide an opportunity for one-on-one interaction with a police officer or a Q&A session with an interpreter onsite: Daly City, East Palo Alto, Redwood City, San Bruno, City of San Mateo, South San Francisco, and the San Mateo County Sheriff’s Office.

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F7. Of the seven law enforcement agencies listed in F6, six provide publication information in more than English: Daly City, East Palo Alto, Redwood City, City of San Mateo, South San Francisco, and the San Mateo County Sheriff’s Office.

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F8. Of the seven law enforcement agencies listed in F6, five sponsor specific outreach events for non-English speaking residents: East Palo Alto, Redwood City, City if San Mateo, South San Francisco and the San Mateo County Sheriff’s Office.
Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F9. Of the seven law enforcement agencies listed in F6, six work with other police agencies to reach non-English speaking residents for outreach events: East Palo Alto, Redwood City, San Bruno, City of San Mateo, South San Francisco and the San Mateo County Sheriff’s Office.

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F10. Of the seven law enforcement agencies listed in F6, six provide outreach materials in languages other than English: Daly City, East Palo Alto, Redwood City, San Bruno, South San Francisco, and the San Mateo County Sheriff’s Office.

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

F11. Of the seven law enforcement agencies listed in F6, six provide on-site interpreters for outreach programs: East Palo Alto, Redwood City, San Bruno, City of San Mateo, South San Francisco, and the San Mateo County Sheriff’s Office.

Response: The City of Brisbane agrees with this finding. We have no reason to disagree with the information contained in the Grand Jury’s report.

The San Mateo County 2016-2017 Grand Jury makes the following recommendations to the City Councils of the cities of San Mateo County:

R1. All law enforcement agencies in San Mateo County shall modify their website by including multilingual translation capability to potentially increase access and participation in outreach programs by non-English speaking residents by December 31, 2017.

Response: This recommendation has already been implemented. The Brisbane Police Department and the City of Brisbane website already include multilingual translation capabilities. We provide access to multiple languages via a direct link through Google translate. This link was listed at the bottom of our homepage and not easily accessible. We have now moved the direct Google translate link to the top of the page to make it visible to anyone accessing our website.

The Brisbane Police Department prides itself on the various languages spoken by members of the police department. We employ 7 bilingual officers who are fluent in Spanish, Cantonese, Chinese, and Tagalog.
R2. The law enforcement agencies (Atherton, Brisbane, Colma, and Hillsborough) whose websites lack information about their outreach programs, shall update their website with the outreach programs available on the home page or provide a prominent link to the outreach programs page, by December 31, 2017.

Response: This recommendation has already been implemented. The Brisbane Police Department website has been updated and now contains a current list of all the outreach programs that we provide to our residents and/or business community on our website page.

On behalf of the City of Brisbane, I would like to thank the members of the San Mateo County Grand Jury members for their efforts.

Sincerely,

Lori S. Liu
Mayor
City of Brisbane
cc: San Mateo Grand Jury
    City Clerk
September 12, 2017

Honorable 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

Re: A Delicate Balance: Privacy vs. Protection

Dear Judge Davis,

We are in receipt of the Grand Jury’s final report “A Delicate Balance: Privacy vs. Protection.” Pursuant to your request for response, the Daly City, City Council held a public meeting on September 11, 2017 and approved this response. The City of Daly City responds to the Grand Jury’s findings, conclusions and recommendations as follows:

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: The City neither agrees nor disagrees with this finding. The City is not intimately familiar with local ordinances in other jurisdictions regarding surveillance technology and does not have enough information to comment on this finding.

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: The City agrees it has not enacted any ordinances governing the acquisition and use of surveillance technology, or the accessibility or management of the information acquired. However, the City has signed a records sharing and data retention agreement for warehousing...
data with the Northern California Regional Intelligence Center (NCRIC). This agreement ensures that data warehoused within the NCRIC is subject to federal standards and guidelines for data retention and sharing that are more stringent than state guidelines.

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: The City agrees that it informs residents about the use of surveillance tools in staff reports. The City is not intimately familiar with the practices in other jurisdictions regarding surveillance technology.

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.

Response: The City agrees that it complies with the law requiring ALPR users to "conspicuously" post a link to the ALPR usage and privacy policy on their websites. The City is not intimately familiar with the practices in other jurisdictions regarding surveillance technology.

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 is helpful to residents.

Response: The City disagrees with this finding and believes that the ALPR links provided on the Police Department web page are both specific and helpful to residents. The City is not intimately familiar with the practices in other jurisdictions regarding surveillance technology.
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: 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 City 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:

- 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.

Response: The City believes this request to be reasonable for tools used in the conduct of basic police business such as Body Worn Cameras and ALPRs. Furthermore, the City 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.

However, this recommendation will not be implemented for law enforcement investigative tools and techniques primarily used for complex criminal investigative purposes. It is neither appropriate nor reasonable for law enforcement agencies to publicly explain and
expose certain critical investigative techniques or technology in any type of public forum. Nor would law enforcement agencies seek public input or conduct feedback surveys from the public on the specialized tactics and techniques employed within the criminal justice system designed to detect criminal activity. Checks and balances already exist through the legal system 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.

Public discussion of law enforcement technologies and investigative techniques would be detrimental to ongoing criminal investigations, compromise capabilities to protect communities, and allow individuals involved in criminal activity to more easily avoid detection.

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: 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.

This recommendation will not be implemented because it is not warranted or reasonable. The recommendation contains obstacles that would limit law enforcement’s ability to adapt and evolve to criminal activity and would compromise the safety and security of residents. Law enforcement agencies are unable to wait for regularly scheduled public meetings of their governing bodies while in pursuit of criminals and crimes in progress. Existing state law protects law enforcement agencies from having to disclose investigative, intelligence and security records under the California Public Records Laws.
Government Code 6254 (f) recognizes the need for discretion and protects law enforcement agencies from disclosing investigative and tactical information that would compromise our crime fighting capabilities. Existing laws also prohibit the release of information derived from, or related to the security of our technology systems specifically to ensure those upholding and protecting the public are not compromised.

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.

The City of Daly City appreciates the opportunity to provide written responses to the San Mateo County Civil Grand Jury Report “A Delicate Balance: Privacy vs. Protection.”

Should the Grand Jury require any additional information, please contact me directly at 650-991-8127.

Sincerely,

[Signature]
Patricia E. Martel
City Manager

cc: City Council
    Annette Hipona, City Clerk
    Rose Zimmerman, City Attorney
September 12, 2017

Honorable 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


Dear Judge Davis:

Thank you for the opportunity to review and comment on the above referenced Grand Jury Report filed on July 12, 2017. On September 11, 2017, the Hillsborough City Council held a public meeting and approved the following responses to the Grand Jury Report findings and recommendations listed below.

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.

_The Town of Hillsborough 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.

_The Town of Hillsborough agrees with this finding, relying on the Grand Jury’s representations in their report._

F3. The County, cities and towns 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

The Town of Hillsborough agrees with this finding, relying on the Grand Jury’s representations in their report.

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.

The Town of Hillsborough 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 is helpful to residents.

The Town of Hillsborough does not agree with this finding and believes that the policy posted on the Police Department web page is both specific and helpful to residents. The Town of Hillsborough is not intimately familiar with the practices in other jurisdictions regarding surveillance technology.

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

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 Hillsborough 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.

The Town of Hillsborough 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 Hillsborough 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 Town 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 of Hillsborough does not agree with this finding and believes that the policy posted on the Police Department webpage is both specific and helpful to residents. The Town is not intimately familiar with the practices in other jurisdictions regarding surveillance technology and 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.

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 summary, the Town of Hillsborough 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 of Hillsborough nonetheless rigorously adheres to existing legal constraints to ensure that both public safety and personal privacy are protected.

Respectfully,

[Signature]

Marie Chuang
Mayor
Town of Hillsborough
September 12, 2017

The Honorable 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  


Dear Judge Davis:

The Menlo Park City Council received the above-referenced San Mateo County Civil Grand Jury Report in July of 2017. The report identifies certain findings and recommendations, and requests that the City Council respond in writing to those findings no later than October 10, 2017. On September 12, 2017, the Menlo Park City Council held a public meeting and approved this response.

Regarding the “findings” of the San Mateo County Civil Grand Jury, Council is requested to respond with one of the following:

1. Council agrees with the finding.
2. Council disagrees wholly or partially with the finding, in which case the response shall specify the portion of the finding that is disputed and shall include an explanation of the reasons thereafter.

Regarding the “recommendations” of the San Mateo County Civil Grand Jury, Council is requested to report one of the following actions:

1. The recommendation has been implemented, with a summary regarding the implemented action.
2. The recommendation has not yet been implemented, but will be implemented in the future, with a time frame for implementation.
3. The recommendation requires further analysis, with an explanation and the scope and parameters of an analysis or study, and a time frame for the matter to be prepared for discussion by the officer or director of the agency or department being investigated or reviewed, including the governing body of the public agency when applicable. This time frame shall not exceed six months from the date of the publication of the Grand Jury report.
4. The recommendation will not be implemented because it is not warranted or reasonable with an explanation therefore.
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

The City of Menlo Park agrees with this finding.

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

The City of Menlo Park disagrees wholly with this finding. On May 13, 2014, the Menlo Park City Council passed Ordinance #1007, which added Chapter 2.56 to Chapter 2 of the Menlo Park Municipal Code. This new chapter, entitled Public Safety Information, deals specifically with: Automated License Plate Reader (ALPR) Data Use, Prohibited Use of ALPR Data, ALPR Auditing and Reporting, Public Safety Camera System Data Use, Prohibited Use of Public Safety Camera System and Data, Public Safety Camera System Auditing and Reporting and Adoption of Department Policies. A copy of the ordinance is attached hereto.

This ordinance was enacted after the Menlo Park Police Department, at the urging of local residents dealing with ongoing gang violence, requested the purchase of this technology which included ALPR’s for three police vehicles and neighborhood surveillance cameras mounted at four intersections, to combat crime. Although the purchase was approved in 2013, some council members expressed privacy concerns and wished to be involved in policy development for use and auditing of data collected by these devices. A council “privacy” subcommittee was formed and after several meetings both an ordinance and a resolution were created. These items came to the Council for consideration and there was a great deal of public comment and a very robust debate reading privacy issues. Ultimately, the City Council voted to enact the above-mentioned ordinance.

F3. The County and cities in San Mateo County do inform residents about the use of some surveillance tools (ALPRs 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 meetings 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.

Response

The City of Menlo Park agrees with this finding.

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 website.

Response

The City of Menlo Park agrees with this finding.

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 is helpful to residents.

Response

The City of Menlo Park agrees with this finding.

Recommendations:

The Civil Grand Jury recommends to the City Councils of the Cities of San Mateo County that:

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 simple 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
The recommendation has been implemented. As stated in the Civil Grand Jury Report, although this information is available on the City of Menlo Park Police website, a specific search must be done in order to locate all the ordinances, municipal codes, policies and privacy information regarding surveillance and investigative tools. The Menlo Park Police Department is also one of the only agencies in the region which provides a copy of its entire policy manual online; but as stated above, a specific search must be done in order to locate those policies dealing with surveillance and investigative tools.

The City of Menlo Park Police Department will complete the following changes and modifications to its website by December 31, 2017:

- A link titled “Surveillance and Investigative Tools and Privacy” will be added prominently to the home page of the City of Menlo Park Police webpage.
- This linked page will have a general description of the type of technology used by the police department and provide links to each of these diverse tools that are in use. These links will be for the following tools: ALPRs, Body Worn Cameras and Neighborhood Surveillance Cameras.
- Each linked page for the above tools will include a description of the tool and how it is used. All relevant ordinances, municipal codes, and policies will be available via links. These documents will address each of the above points of information in the recommendation along with a FAQ document about the specific tool.

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 to address those concerns in public meetings, Town Halls, Neighborhood Watch sessions and other local gatherings.
- Using social medal platforms such as Nextdoor to keep residents engaged and informed about surveillance technologies and its uses in your community.

Response
This recommendation has already been implemented. As stated in the above response to Finding 2, when ALPRs and neighborhood surveillance cameras were purchased, a robust public debate occurred prior to implementation. This debate
included numerous City Council meetings, town hall meetings, and social media notification along with a specific subcommittee formed by the City Council to address privacy issues. As a result of this vigorous debate, Menlo Park Ordinance 1007 was adopted.

In 2011, City Council approved the purchase of body worn cameras for a period of "beta" testing. In 2012, City Council approved the purchase of Body Worn Cameras for the entire police department. At that time there was healthy public debate at numerous City Council meetings, town hall meetings, and social media notification regarding privacy, the use of the cameras and storage of data. City Council directed the police department to confer with community members along with the Police Chief’s Advisory Board in order to address these issues and create a police department policy. Several draft policies were created which were presented at several City Council meetings, where council members raised questions and concerns and requested changes to the policy. In 2015 a final and adopted policy on the use of body worn cameras was completed and presented to council.

While the City Council was satisfied with the policy overall as it dealt with privacy, a concern was raised about the retention period of the data collected by the cameras. Due to this concern, the Police Department created an "Audio/Video Recording Destruction Request and Waiver". This new waiver and procedure allows a member of the public, under certain circumstances, to request a recording of a non-event to be destroyed after one year, prior to the 2.5 year retention period established by policy. This was yet another example of the serious consideration to privacy issues addressed by the City of Menlo Park.

The City of Menlo Park will follow the above example of public disclosure and discussion prior to the purchase and implementation of any new surveillance technology that is considered by the police department.

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 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

This recommendation has already been implemented. As stated above, each of the
listed surveillance tools in use by the police department were completely vetted by the City Council and the public and each privacy issue was addressed. It should also be noted that in regard to point #3 above, Ordinance 1007 passed by City Council, requires the police department to provide bi-annual reports on the use of the ALPR technology.

Sincerely,

[Signature]

Kirsten Keith
Mayor, City of Menlo Park

Enclosure
The City Council of the City of Menlo Park does ordain as follows:

SECTION 1. FINDINGS AND DETERMINATIONS. The City Council of the City of Menlo Park hereby finds and declares as follows:

A. The Menlo Park Police Department has acquired Automated License Plate Readers to be installed on one or more Police Department vehicles to be used by the Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen and wanted vehicles, stolen license plates and missing persons, and to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

B. The City of Menlo Park plans to operate a Public Safety Camera System for the purpose of creating a safer environment for all those who live, work and visit the City, which cameras may be used for detecting and deterring crime, to help safeguard against potential threats to the public, to help manage emergency response situations during natural and man-made disasters and to assist City officials in providing services to the community.

C. The City Council is concerned about protecting the privacy of its residents with respect to the retention and use of data obtained by Automated License Plate Readers and the Public Safety Camera System and desires to add Chapter 2.56 [Public Safety Information] to Title 2 [Administration and Personnel] of the Menlo Park Municipal Code to address the use and retention of this information.

SECTION 2. ADDITION OF CODE. Chapter 2.56 [Public Safety Information] is hereby added to Title 2 [Administration and Personnel] of the Menlo Park Municipal Code to read as follows:
Chapter 2.56
PUBLIC SAFETY INFORMATION

Sections:

2.56.010 Purpose
2.56.020 Definitions
2.56.030 Automated License Plate Reader Data Use
2.56.040 Prohibited Use of Automated License Plate Reader and Data
2.56.050 Automated License Plate Reader Auditing and Reporting
2.56.060 Public Safety Camera System Data Use
2.56.070 Prohibited Use of Public Safety Camera System and Data
2.56.080 Public Safety Camera System Auditing and Reporting
2.56.090 Adoption of Department Policies

2.56.010 Purpose

The purpose of this Chapter is to provide for the proper use of data and recordings gathered by the City through the use of Automated License Readers and the Public Safety Camera System.

2.56.020 Definitions

For the purposes of this Chapter, the following words and phrases shall have the meanings ascribed to them in this Section:

A. "Automated License Plate Reader" or "ALPR" means technology, also known as License Plate Recognition, which provides automated detection of license plates.

B. "Data" means information gathered by the Automated License Plate Reader in the form of license plates and metadata (location and time license plate was viewed).

C. "Public Safety Camera System" means cameras that record images only and not sound and that are placed in strategic fixed locations within the City at the direction of the Chief of Police and with the approval of the City Council for the purpose of detecting and deterring crime, to help emergency services personnel maintain public order, to help manage emergency response situations during natural and man-made disasters, to monitor pedestrian and vehicle traffic activity, to assist in the preparation of traffic reports, and to assist City officials in prosecuting and/or defending civil or administrative actions.

D. "Recordings" means the recorded images, without sound, recorded by the Public Safety Camera System.
2.56.030 Automated License Plate Reader Data Use

A. Data will be securely transmitted to the Northern California Regional Intelligence Center ("NCRIC") as part of a multi-jurisdictional 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, provided NCRIC has executed an agreement with the City agreeing to comply with the retention/destruction provisions set forth in this section.

B. Data transmitted to NCRIC from the Police Department shall be kept no more than six months, and then destroyed, unless retention of specific identified license plate data is necessary for an active criminal case or pursuant to a valid court order.

C. Data may only be accessed by law enforcement personnel who are approved to access the data and who have undergone required NCRIC training for legitimate law enforcement purposes only, such as when the data relates to a specific criminal investigation or department-related civil or administrative action.

D. Data may be accessed by other NCRIC agencies that have executed a Memorandum of Understanding with NCRIC, but only for legitimate law enforcement purposes and by authorized/trained personnel and only in compliance with all policies, procedures and reporting requirements of NCRIC.

E. Data may be released to other non-NCRIC authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes, with approval of the Chief of Police or Police Commander, provided any such official and/or agency has executed an agreement with the City agreeing to comply with the terms and provisions of Sections 2.56.030 and 2.56.040.

F. All data and images gathered are for official use of the Police Department and because such data may contain confidential California Law Enforcement Telecommunications Systems ("CLETS") information, it is not open to public view or inspection.
2.56.040 Prohibited Use of Automated License Plate Reader and Data

A. ALPR shall not be used to invade the privacy of individuals, to look into private areas or areas where the reasonable expectation of privacy exists, nor shall they be used to harass, intimidate or discriminate against any individual or group, nor for any purpose not specifically authorized by this Chapter.

B. Unauthorized access, possession or release of data is a violation of Police Department policy and various federal and state criminal statutes. Any employee, who accesses, possesses or releases data, from the ALPR database without authorization or in violation of this Chapter and such additional policies established by the Police Department, may face department discipline up to and including termination, criminal prosecution and/or civil liability.

2.56.050 Automated License Plate Reader Auditing and Reporting

A. NCRIC will give a quarterly report to the Police Department which shall indicate the number of license plates captured by the ALPR in the City of Menlo Park, how many of those license plates were “hits” (on an active wanted list), the number of inquiries made by Menlo Park personnel along with the justifications for those inquiries, and information on any data retained beyond six months and the reasons for such retention in compliance with Section 2.56.030B.

B. Following receipt of the NCRIC report described in subsection A., above, the Police Department shall provide an information report to the City Council.

C. ALPR system audits will be randomly conducted by the California Department of Justice and in conjunction with yearly CLETS audits.

2.56.060 Public Safety Camera System Data Use

A. Public safety camera recordings may only be used for the purpose of criminal investigations, detecting and deterring crime, to help emergency services personnel maintain public order, to help manage emergency response situations during natural and man-made disasters, to monitor pedestrian and vehicle traffic activity, to assist in the preparation of traffic accident reports, and to assist City officials in prosecuting and/or defending civil or administrative actions.

B. Recordings will be made in a professional, ethical and legal manner.
C. All recordings will be stored by the Police Department in a secure area with access restricted to authorized persons, and shall not be accessible by third parties without express permission.

D. Recordings not otherwise needed for reasons in subsection A. shall be retained for a period of up to 90 days and then erased or recorded over as limited by the storage capacity of the cameras.

E. Any recordings needed as evidence in a criminal or civil case proceeding or for another reason specified in subsection A. shall be collected and booked in accordance with current Police Department evidence procedures.

F. Recordings may only be released to other authorized and verified law enforcement officials and agencies for legitimate law enforcement purposes as specified in subsection A. with approval of the Chief of Police or Police Commander, provided such official or agency executes an agreement with the City agreeing to comply with the terms and provisions of Sections 2.56.060 and 2.76.070, or with a valid court order.

G. Except as required by a valid court order or other lawful process, recordings do not constitute public records and will not be disclosed to the public.

H. Facial recognition and cognitive security software may only be used to review recordings from the Public Safety Camera System with the approval of the Chief of Police or Police Commander in specific criminal investigations or specific threats to public safety.

2.56.070 Prohibited Use of Public Safety Camera System and Data

The Public Safety Camera System will not be used to invade the privacy of individuals, to look into private areas or areas where the reasonable expectation of privacy exists. The Public Safety Camera System shall not be used to harass, intimidate or discriminate against any individual or group, nor for any purpose not authorized by this Chapter.

2.56.080 Public Safety Camera System Auditing and Reporting

A. The Chief of Police or his/her designee will conduct an annual review of the Public Safety Camera System, its use, effectiveness and adherence to policy, including frequency and purpose for use of facial recognition or cognitive security software and frequency and purpose for retention of recordings beyond 90 days,
and will provide an annual information report to the City Council regarding such review.

2.56.90 Adoption of Department Policies

The Police Department is directed to adopt policies to be included in its policy manual consistent with the provisions of this Chapter, which policies may be more restrictive, but not less restrictive, than the policies set forth in this Chapter.

SECTION 3. CALIFORNIA ENVIRONMENTAL QUALITY ACT DETERMINATION. The City Council hereby finds that this ordinance is not subject to the provisions of the California Environmental Quality Act ("CEQA") because the activity is not a project as defined by Section 15378 of the CEQA Guidelines. The ordinance has no potential for resulting in physical change to the environment either directly or indirectly.

SECTION 4. SEVERABILITY. If any part of this Ordinance is held to be invalid or inapplicable to any situation by a court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of this Ordinance or the applicability of this Ordinance to other situations.

SECTION 5. EFFECTIVE DATE AND PUBLISHING. This Ordinance shall become effective 30 days after the date of its adoption. Within 15 days of its adoption, the Ordinance shall be posted in three public places within the City of Menlo Park, and the Ordinance, or a summary of the Ordinance prepared by the City Attorney shall be published in the local newspaper used to publish official notices for the City of Menlo Park prior to the effective date.

INTRODUCED on the 13th day of May, 2014.

PASSED AND ADOPTED as an Ordinance of the City of Menlo Park at a regular meeting of the City Council of the City of Menlo Park on the 3rd day of June, 2014, by the following vote:

AYES: Cline, Keith, Mueller
NOES: Carlton, Ohtaki
ABSENT: None
ABSTAIN: None

ATTEST: Pamela Aguilar
City Clerk

APPROVED: Ray Mueller
Mayor
July 18, 2017

The Honorable 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

Reference:  Response to the Grand Jury Report – A Delicate Balance: Privacy vs. Protection

Dear Judge Leland Davis, III:

As you are aware, the City of Millbrae contracts for law enforcement services with the San Mateo County Sheriff's Office. The Privacy vs. Protection report is a topic we have discussed with the Sheriff's Office. In fact prior to the Grand Jury report, the Sheriff held two community meetings to discuss the topic of Automated License Plate Readers.

The Sheriff realizes the importance of meeting the community needs in determining what the acceptable conditions are for the use of surveillance methods. Therefore, we would expect the Sheriff to continue to meet with the community regarding the specific recommendations made by the Grand Jury.

I want to thank you for the work the Grand Jury did. In today’s environment it is important for law enforcement to break down barriers and continue to expand their outreach to growing diverse communities.

Sincerely,

Marcia Raines
City Manager
July 27, 2017

Grand Jury Foreperson
c/o Court Executive Officer
400 County Center
Redwood City, CA 94063-1655

Re: Response to Grand Jury Report
A Delicate Balance: Privacy vs. Protection

Dear Grand Jury Foreperson:

The Town Council for the Town of Portola Valley ("Town") has reviewed the recommendations in the Grand Jury Report "A Delicate Balance: Privacy vs. Protection" and approved the following responses at the public meeting on July 26, 2017:

**Recommendation No. 1**
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 No. 1**
The Town contracts with the San Mateo County Sheriff's Department for law enforcement services. Therefore, the Town is not in a position to implement this recommendation. The Town will cooperate with the Sheriff's Department, as necessary, to implement the recommendation. Additionally, after a robust public process, on April 26, 2017, the Town Council of the Town of Portola Valley adopted Ordinance No 2017-418 adding Chapter 9.02, Public Safety Information, to the Town's Municipal Code. This ordinance, which addresses the use and retention of ALPR data, and related materials are readily available on the Town's website.
Recommendation No. 2
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.

Response No. 2
The Town contracts with the San Mateo County Sheriff’s Department for law enforcement services. Therefore, the Town is not in a position to implement this recommendation. The Town will cooperate with the Sheriff's Department, as necessary, to implement the recommendation. Additionally, after a robust public process, on April 26, 2017, the Town Council of the Town of Portola Valley adopted Ordinance No 2017-418 adding Chapter 9.02, Public Safety Information, to the Town's Municipal Code. The robust public process included a number of public meetings over a two-year period prior to adoption of the use of ALPR technology in town.

Recommendation No. 3
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 No. 3
The Town contracts with the San Mateo County Sheriff’s Department for law enforcement services. Therefore, the Town is not in a position to implement this recommendation. The Town will cooperate with the Sheriff’s Department, as necessary, to implement the recommendation. Additionally, after a robust public process, on April 26, 2017, the Town Council of the Town of Portola Valley adopted Ordinance No 2017-418 adding Chapter 9.02, Public Safety Information, to the Town's Municipal Code. The robust public process included a number of public meetings over a two-year period prior to adoption of the use of ALPR technology in town.

The Town thanks the Grand Jury for bringing this issue to our attention in an informative and thorough manner. Please let me know if you require additional information.
Sincerely,

Craig Hughes
Mayor

cc: Town Council
    Town Manager
    Town Attorney
September 12, 2017

Honorable 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
(Sent via email)


Dear Judge Davis:

On behalf of the City Council of the City of Redwood City, I would like to thank you for the opportunity to respond to the Grand Jury Report released on July 12, 2017, entitled “A Delicate Balance: Privacy vs. Protection.” The following response to the Grand Jury Report was reviewed and approved by the City Council at its meeting on September 11, 2017.

Pursuant to Penal Code § 933.05, the Grand Jury requested response from the City of Redwood City on Recommendations 1, 2, and 3. The Recommendations and the City’s responses are detailed as follows:

**Recommendation 1:** 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.

**Partially Agree:** As required by law, the City has already posted on the City website the operational policy governing the use of ALPR technology. The City will post operational policies for additional surveillance equipment where the release of such information does not unnecessarily jeopardize public safety and criminal investigations. This information will be placed in a conspicuous location on the City’s website by December 31, 2017.

**Recommendation 2:** 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.

**Partially Agree:** The City recognizes that not all of its citizens utilize the internet or social media to stay informed about City business. As resources permit and as warranted by community interest, the City will share information or answer questions related to use of surveillance equipment, governing laws and operational policies in business and neighborhood association meetings, neighborhood watch gatherings, and publicly noticed City meetings.

However, the City believes that law enforcement investigative tools and analytical technologies primarily used for complex criminal investigations should not be subject to this same public disclosure as basic police surveillance equipment. Public discussion on these law enforcement technologies and investigative techniques would be detrimental to ongoing criminal investigations, compromise capabilities to protect our community, and allow individuals involved in criminal activity to more easily avoid detection.

**Recommendation 3:** 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.

Partially Agree: The City agrees to provide the public an opportunity to provide input to the City Council on certain surveillance equipment purchases and to post governing policies on the City's website. The City believes that existing law and City Council review at publicly noticed City meetings provides the public with appropriate oversight when acquiring certain new surveillance equipment, including a process to review governing policies written for the Redwood City Police Department.

However, reporting on the effectiveness of surveillance tools will not be implemented as it would prove to be limiting in the Police Department's ability to adapt and evolve to changing criminal activity. Further, it would serve to alert and provide individuals involved in criminal activity an opportunity to more easily avoid detection or change their method of operation based on the effectiveness or lack thereof of certain surveillance equipment.

The City Council of Redwood City appreciates the work the Grand Jury did in the preparation of this report and the value it places on forging strong relationships between local law enforcement and the diverse communities served within the County of San Mateo.

Sincerely,

[Signature]
John D. Seybert, Mayor
City of Redwood City

Cc: City Council, Redwood City
    Melissa Stevenson Diaz, City Manager
    Gary L. Kirby, Acting Chief of Police
September 12, 2017

Honorable 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


Dear Judge Davis:

In reply to your request for responses to the above referenced report, the City of San Carlos hereby submits this letter, which was approved by the City Council at the September 11, 2017 Council meeting.

Findings.

The City of San Carlos reviewed all five of the Findings in the Grand Jury report. Since the Findings are based on research conducted by the Grand Jury of San Mateo County of San Mateo County agencies, including cities and the San Mateo County Sheriff’s Office, we cannot independently confirm the Findings. However, to respond to your request that we agree with the Findings, we feel we are able to agree with Findings 1-4, but cannot agree with Finding 5. Finding 5 is vague as to what specific information is helpful to residents and no survey of residents in our County has been undertaken concerning surveillance issues to enable the City to agree or disagree with this Finding.

Recommendations.

The City of San Carlos contracts with the San Mateo County Sheriff for Police Services. In consultation with the Sheriff’s Office, the City of San Carlos reviewed the three Recommendations in the Grand Jury report. The City of San Carlos and the Sheriff’s Office will continue to conduct an open public process regarding new surveillance technologies and the Recommendations made will be considered as additional steps when implementing new technologies.

The City of San Carlos appreciates the opportunity to comment on the Grand Jury report.

Best Regards,

Bob Grassilli, Mayor
September 6, 2017

The Honorable 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

Subject: Response of the City of South San Francisco to the Grand Jury Report “A Delicate Balance: Privacy vs. Protection.”

Dear Judge Davis,

Thank you for the opportunity to respond to the Grand Jury report entitled “A Delicate Balance: Privacy vs. Protection.” The City of South San Francisco’s response to both the findings and recommendations are listed below.

Responses 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:
The City of South San Francisco understands what is represented in the Grand Jury Report. The City is not intimately familiar with local ordinances in other jurisdictions regarding surveillance technology, and therefore takes no position on this Finding.

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:
The City of South San Francisco agrees that it has not enacted any ordinances specifically governing the acquisition and use of surveillance technology, or the accessibility, management, or retention of the information acquired. The City does not have enough information regarding other local ordinances within San Mateo County regarding surveillance technology to state a position.
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.

Response:
The City of South San Francisco agrees that it informs residents about the use of surveillance tools at public forums and city council meetings. The City is not familiar with the practices in other jurisdictions regarding surveillance technology.

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.

Response:
The City of South San Francisco agrees that it complies with applicable state law requiring ALPR users to "conspicuously" post a link to the ALPR usage and privacy policy on their websites. The City is not familiar with the practices in other jurisdictions regarding surveillance technology.

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:
The City of South San Francisco believes that the policy posted on the South San Francisco Police Department web page is both specific and helpful to residents. However, the South San Francisco Police Department will evaluate the provided information to determine if amendments are necessary. The City is not familiar with the practices in other jurisdictions regarding surveillance technology.

Responses 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:
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 City of South San Francisco 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:

- 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.

Response:
The City of South San Francisco believes this request to be reasonable for tools used in the conduct of basic police business such as Body Worn Cameras and ALPRs. Furthermore, the City of South San Francisco 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.

However, this recommendation will not be implemented for law enforcement investigative tools and techniques primarily used for complex criminal investigative purposes. It is neither appropriate nor reasonable for law enforcement agencies to publicly explain and expose certain critical investigative techniques or technology in any type of public forum. Nor would law enforcement agencies seek public input or conduct feedback surveys from the public on the specialized tactics and techniques employed within the criminal justice system designed to detect criminal activity. Checks and balances already exist through the legal system 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.

Public discussion of all law enforcement technologies and investigative techniques would be detrimental to ongoing criminal investigations, compromise capabilities to protect communities, and allow individuals involved in criminal activity to more easily avoid detection.

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

However, this recommendation will not be implemented because it is not warranted or reasonable for law enforcement agencies to disclose reports on the effectiveness of surveillance tools. To do so would create obstacles that would limit law enforcement’s ability to adapt and respond to criminal activity and would compromise the safety and security of residents. Furthermore, existing state law protects law enforcement agencies from having to disclose investigative, intelligence and security records under the California Public Records Act.

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

Under California Penal Code Sections through 1546 through 1546.4, known as the Electronic Communications Privacy Act, law enforcement is required to obtain court orders related to electronic communications intercept surveillance. Furthermore, California Penal Code Sections 1524 and 1534 require court orders for the use of electronic tracking devices.

Sincerely,

Mike Furell
City Manager