August 4, 2016

VIA EMAIL ONLY

Deputy Chief Benson H. Fairow (bfairow@bart.gov)
Matthew H. Burrows (mburrow@bart.gov)
Russell G. Bloom (rbloom@bart.gov)
Byron Toma (btoma@bart.gov)
Bay Area Rapid Transit District
300 Lakeside Drive
Oakland, CA 94612

Re: Automated License Plate Readers (ALPR)

Dear Deputy Chief Fairow:

Thank you for the opportunity to comment on the proposed Bay Area Rapid Transit ("BART") ALPR policy. As a member of Oakland Privacy ("OP"), and chair of the Privacy Advisory Commission at Oakland's City Hall, I appreciate that BART is addressing community concerns related to the use of surveillance equipment in a good faith and transparent manner.

OP is a citizen's coalition that works regionally to defend the right to privacy and enhance public transparency and oversight regarding the use of surveillance techniques and equipment. We were instrumental in the creation of the first standing municipal citizens' privacy advisory commission in the City of Oakland, and we have engaged in successful privacy enhancing legislative efforts with the Counties of Alameda and Santa Clara. In 2015, we successfully urged the California State Legislature to pass SB 34, which now regulates the use of ALPR throughout the state.

BART'S ALPR POLICY DOES NOT COMPLY WITH SB 34

As a threshold issue, it must be noted that SB34 has no exceptions for trial use of ALPR. The current draft policy bulletin states that a formal policy "will be issued" if ALPR is adopted long-term. The length of ALPR use is irrelevant to BART's compliance with SB34.

Pursuant to Cal. Civil Code, §1798.90.53(b)(2), BART'S ALPR policy must at minimum contain the following:

> *(B) A description of the job title or other designation of the employees and independent contractors who are authorized to access and use ALPR information. The*

> *policy shall identify the training requirements necessary for those authorized employees and independent contractors.*

The BART policy states that the Support Services Deputy Chief will assign personnel under his/her command to operate and use ALPR. The above section does not require or seek information related to who may authorize use. Rather, it requires information about who is authorized to perform such use. In addition, the policy fails to "identify" the training requirements necessary for authorized members to use BART ALPR, only stating that department-approved training must be completed.

> *(C) A description of how the ALPR system will be monitored to ensure the security of the information accessed or used, and compliance with all applicable privacy laws and a process for periodic system audits.*

The BART policy does not address compliance with applicable privacy laws, nor describe a process for periodic system audits. In fact, the policy does not even require audits, only saying they "should" occur, rather than "shall". See Accountability And Safeguards (e).

> *(D) The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons.*

We have informally discussed our objection to the automatic uploading of ALPR data collected by BART to databases such as NCRIC or ARIES absent any legitimate need to do so, and we again state our objection here.

The BART policy should be revised to mandate a "need to know" concept that we have successfully introduced in other jurisdictions, regardless of NCRIC participation. A major concern of the public since the Edward Snowden revelations is the unrestricted sharing of data between law enforcement agencies, for no apparent law enforcement purpose. With the use policies OP has had a direct involvement in drafting, governing bodies throughout the Bay Area have seen the wisdom in requiring that a direct involvement in the investigatory process be present in order to obtain data, as opposed to unrestricted use and sharing through NCRIC as contemplated by the BART policy. We see no compelling reason that all sworn officers within your department be provided access to this data without a demonstrated need for it, let alone all law enforcement statewide[1]. If they do not have a direct role in the investigation, an officer should be prohibited from accessing the data. See also Accountability And Safeguards (d). In Oakland's use policies, "need to know" is defined as:

> "Need To Know" means even if one has all the necessary official approvals (such as a security clearance) to access the [ALPR], one shall not be given access to the [ALPR] or [ALPR] Data unless one has a specific need to access the system or data in order to conduct one's official duties in connection with one of the [allowable uses in this policy.]

[1] NCRIC, the Northern California Regional Intelligence Center, is a federally funded "fusion center" located in San Francisco, and its jurisdiction essentially encompasses the entire state of California.

Bay area residents have legitimate concerns about the wholesale transfer of their data into a national homeland security fusion center every time they park a vehicle at McArthur BART. At the earlier ALPR meeting before the Board that initiated this discussion, several BART directors indicated that BART has the capacity to store ALPR data internally without uploading to NCRIC. Oakland, Berkeley, Tiburon, Hayward, and San Jose police departments do not share data with NCRIC, for but a few examples. If the Board sees participation in NCRIC as desirable, then OP recommends adoption of the California Highway Patrol's data retention limits of 60 days as mandated by state law, and which provides a guideline to BART regarding retention of ALPR data for transit-focused agencies.

> *(E) The title of the official custodian, or owner, of the ALPR information responsible for implementing this section.*

The BART policy fails to address this requirement.

> *(F) A description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors.*

The BART policy fails to address how incorrect data errors will be corrected. Recent legal action against the City of San Francisco by a woman wrongfully detained at gunpoint pursuant to an incorrect license plate scan shows the wisdom of ensuring accuracy in license plate images. After losing its legal appeal, in 2015 the City of San Francisco paid Denise Green $495,000 for this very costly mistake.[2] The ALPR 'hit' was inaccurate by only one digit, yet the consequences were enormous. For an ongoing local example of ALPR's inherent inaccuracy, one has only to look at the quarterly ALPR reports produced by Menlo Park, where the vast majority of 'hits' are proven to be false reads[3].

> *(G) The length of time ALPR information will be retained, and the process the ALPR end-user will utilize to determine if and when to destroy retained ALPR information.*

In a previous discussion, you indicated that BART would consider reducing the length of retention from one year to six months. We appreciate this acknowledgment of the impact to privacy that location-tracking data such as ALPR has. In order to reduce risk of misconduct, OP believes that the data should be destroyed the instant there is no demonstrated need for it. We address retention limits further below.

RETENTION OF DATA MUST BE DETERMINED BY NEED

The existing policy authorizes the storage of license plate scans for one year. While unstated in the policy, it is likely that BART cannot justify this position. BART has not publicly produced any metrics or evidence showing the need for retention of any length, let alone six months to a year. There is no legal requirement that data be retained for any length of time. Tiburon keeps its data no longer than 100 days, unless required for an active investigation.[4] Oakland and Menlo Park keep their data for 6

[2] https://sfgov.legistar.com/View.ashx?M=F&ID=4094981&GUID=5940D244-9174-41E7-A442-BF1046C986B1
[3] http://www.menlopark.org/DocumentCenter/View/9590
[4] http://www.townoftiburon.org/DocumentCenter/View/697, Section 461.5 Accountability and Safeguards

months.[5][6] State law requires that the California Highway Patrol delete its data after 2 months.[7]

The longer data is retained, the more likely it is that an invasion of privacy will occur, that data will be misused or stolen by hackers, and costs of storage will certainly increase. While a single data point may not intrude greatly upon our right to privacy, the likelihood of infringement increases as more data points are accumulated and retained. A mosaic, or pattern, emerges as to one's travel and associations. As data from various systems and containing different sorts of information is uploaded to law enforcement databases like ARIES and NCRIC without careful thought, the ability of law enforcement to access a very revealing portrait of our lives should give BART pause before granting such power to its police department. After a reporter correctly figured out where he lived based solely on Oakland's ALPR data, Oakland Councilmember Dan Kalb stated that he believed that the purpose of ALPR was only to track down stolen vehicles. "It raises the question: what's the purpose of retaining records for a long period of time?"[8] OP believes this question should be asked by BART prior to possibly authorizing ALPR use, and when discussing retention limits.

The annual reporting metrics suggested in the section below can also provide guidance here as to the appropriate retention time. As efficacy data is collected, the Directors can make amendments to the policy if a different retention time is needed. Comparing license plate images to a Hot List database takes but a second. If the image is not a 'hit', what is the justification for retaining the ALPR data, which could include photos of people and other personal information?[9] Absent reasonable suspicion that the observed license plate belongs to a vehicle owner suspected of a crime, or that the vehicle itself was involved in a crime, OP sees no compelling reason that ALPR data of people suspected of no wrongdoing be retained.

The International Association of Chiefs of Police acknowledges the civil liberties implications from ALPR use:

> "Recording driving habits could implicate First Amendment concerns. Specifically, LPR systems have the ability to record vehicles' attendance at locations or events that, although lawful and public, may be considered private. For example, mobile LPR units could read and collect the license plate numbers of vehicles parked at addiction counseling meetings, doctors' offices, health clinics, or even staging areas for political protests."[10]

In order to minimize the potential for unconstitutional policing and infringement upon our right to privacy, BART should seek to minimize the collection *and* retention of data, to the least amount possible.

---

[5] http://arstechnica.com/tech-policy/2015/08/cops-decide-to-collect-less-license-plate-data-after-80gb-drive-got-full/
[6] http://www.codepublishing.com/CA/MenloPark/?MenloPark02/MenloPark0256.html&?f, Section 2.56.030(b)
[7] Cal. Vehicle Code, §2413(b)
[8] http://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/2/
[9] Please see the attached ALPR photo of OP member Mike Katz-Lacabe, produced to him via public record request.
[10] "Privacy impact assessment report for the utilization of license plate readers", International Association of Chiefs of Police, September 2009, page 2.

REPORTING METRICS ENABLE BART DIRECTORS TO MAKE INFORMED DECISIONS

As with any tool, measuring the effectiveness of use is important for both taxpayer and civil liberties concerns. How will BART demonstrate effectiveness, when its policy fails to include any metrics or efficacy reports? OP recommends that measurable reporting statistics be included in a required annual report to the Directors. BART's future SB 34-compliant ALPR policy should include in its annual report a category for total costs, including ongoing maintenance and support, personnel, licensing, and any other related cost, and a summary of uses and results of any criminal investigations, so that the Directors can make an informed decision as to whether continued use is justified. Tiburon's ALPR policy requires that its chief of police present an annual report that includes annual system costs and also a summary of any policy violations. See Tiburon ALPR Policy, Section 461.9. All of Oakland's use policies have robust efficacy metrics and a required annual report.

REASONABLE SUSPICION MUST BE REQUIRED

The BART policy states that neither the reasonable suspicion nor probable cause standards are required to utilize ALPR. OP strongly disagrees with this position. When law enforcement acts without at least a reasonable suspicion that criminal wrongdoing has occurred, the door is opened to civil liberties infringement including upon our right to privacy, and to targeting and profiling of innocent citizens that lacks a rational and defined basis. Communities across the country have been expressing resistance to undefined targeting by law enforcement, most notably in the New York City stop-and-frisk policy that was ruled unconstitutional.[11] OP would be happy to work with BART to develop language that protects privacy and civil liberties, without preventing law enforcement from lawfully investigating suspected crime. In the current policy, an amendment could be made to ALPR Operation (a):

"An ALPR shall only be used for official and legitimate law enforcement business and pursuant to Reasonable Suspicion that an unlawful act has occurred." Elsewhere in the policy, reasonable suspicion should be defined. In Oakland's use policies, we used the following definition:

> "Reasonable Suspicion" means specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch that an individual or organization is involved in a definable criminal activity or enterprise. Reasonable Suspicion shall not be based on Protected Activity. Furthermore, a suspect's actual or perceived race, national origin, color, creed, age, alienage or citizenship status, gender, sexual orientation, disability, or housing status, shall not be considered as a factor that creates suspicion, and may only be used as identifying information in the description of a criminal suspect.

CONCLUSION

Modern technology has introduced a host of new challenges in navigating the balance between security and freedom. OP believes these challenges are best met with a public conversation between elected leaders and their constituents, which examines the potential impact to privacy and all civil liberties from use of surveillance equipment. If we can provide any supplementary information or assistance

11 http://ccrjustice.org/home/press-center/press-releases/landmark-decision-judge-rules-nypd-stop-and-frisk-practices

with BART's privacy policy for ALPR implementation, please do not hesitate to contact us.

Brian Hofer
510-303-2871
Oakland Privacy
E-Mail: contact@oaklandprivacy.com
E-Mail: brian.hofer@gmail.com
Web: oaklandprivacy.org

cc:

Dir. Nick Josefowitz (nick.josefowitz@bart.gov)
Dir. Joel Keller (joel.keller@bart.gov)
Dir. Rebecca Saltzman (Rebecca.saltzman@bart.gov)
Dave Maas (dm@eff.org)
Matt Cagle (mcagle@aclunc.org)