



VIA EMAIL

August 7, 2018

Hon. Rebecca Saltzman (rebecca.saltzman@bart.gov)
Hon. Robert Raburn (robert.raburn@bart.gov)
Hon. Debora Allen (Deborah.allen@bart.gov)
Hon. Joel Keller (joel.keller@bart.gov)
Hon. John McPartland (boardofdirectors@bart.gov)
Hon. Thomas Blalock (boardofdirectors@bart.gov)
Hon. Lateefah Simon (lateefah.simon@bart.gov)
Hon. Nick Josefowitz (nickj@getsfmoving.com)
Hon. Bevan Dufty (bevan.dufty@bart.gov)

Re: Safety & Security Action Plan – PSIM and Camera Expansion/Conversion

Dear Honorable Directors:

On behalf of Oakland Privacy, I write to urge you to **reject** the staff proposals pertaining to procurement of a Physical Security Information Management System (“PSIM”) and upgrading of system cameras, listed within Agenda Item 5 B, for the below reasons.

OP is a citizens’ 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 privacy enhancing legislative efforts with the Counties of Alameda and Santa Clara, and the cities of Oakland, Davis, Berkeley, and Palo Alto.

BART’S BOARD MUST STAY CONSISTENT

On April 28, 2016, the Board did not approve staff’s proposal to install automated license plate readers, tabling the matter until a “global surveillance use policy” could be returned to the Board for its consideration. Community members were invited to participate, and I am one of those privileged members that has spent the past two years drafting said ordinance, along with your staff. In December 2016, the Technology & Communications Committee approved our concept (“Surveillance Equipment Ordinance” or “SEO”), and directed that we continue to work with staff on finding more common ground. We have continued to do so, and as staff represented in its agenda report, we could be ready for Board review in September or October.

As a member of Oakland Privacy (“OP”), and chair of the City of Oakland’s Privacy Advisory Commission, I appreciate that BART is addressing community concerns related to the use of surveillance equipment in a good faith and transparent manner, especially in this political climate where folks of different color, faith, and birthplace are increasingly under attack.

It was quite a shock to read of BART staff’s dramatic plans to expand its surveillance equipment capabilities in the media, without any notice from our working partners. It was additionally frustrating to see that although we had negotiated the language in the SEO and agreed that an Impact Analysis Report and draft Use Policy are required for any surveillance equipment proposal to the Board, neither document was created for the PSIM and camera expansion proposals. In fact, we just received a new draft of the SEO on the day the news broke, without any mention of the PSIM proposal or request for feedback.

While requesting approximately \$25 million in up front funds, with an anticipated \$3 million in annual ongoing costs, and upgrading of 2,000 or more cameras, staff provides no analysis as to how PSIM will increase the public safety of its riders. No proposal of this magnitude should be approved without at least conducting a robust analysis of its impact to our civil liberties and privacy rights, and potential effectiveness and costs, and without review of a draft use policy showing the intended uses, and restrictions on data collection, retention and sharing.

OAKLAND’S PSIM PROBLEMS (DOMAIN AWARENESS CENTER)

Most of you were already familiar with the history surrounding Oakland’s attempted installation of a citywide mass surveillance system, based on a PSIM platform like the one before you, and called the Domain Awareness Center (“DAC”). During the above April ’16 license plate reader discussion, we cautioned BART not to go down the same path as Oakland – by installing equipment prior to considering its impact, or performing community outreach as to the appropriateness of such equipment use. The Board clearly listened then, as it invited Oakland Privacy, the ACLU, and others to work with staff on mitigating any concerns prior to proceeding with a proposal, and you should continue to listen as these concerns have only heightened under Donald Trump and with increased data sharing.

Oakland’s staff worked on the DAC for 3-4 years without any community involvement. When the community became aware of its capabilities, staff and the City Council ran into stiff resistance which generated international headlines. Oakland’s city council wisely tabled the project, tasked a citizen’s task force with crafting a privacy policy (which did not exist in Oakland), and ultimately approved a standing citizen’s privacy commission and an SEO, like the one contemplated for BART. Oakland is now considered the national leader in the defense of civil liberties and our right to privacy, while still allowing for legitimate police work to continue.

Oakland taxpayers were forced to pay for tens of thousands of dollars of unnecessary staff time spent planning the DAC, only to realize the overwhelming majority of the community rejected many of the features the proponents desired, like facial recognition. It was not a good look for Oakland, or its elected leaders, and BART appears to be heading in the same wrong direction. We encourage you to learn from our mistakes, not replicate them.

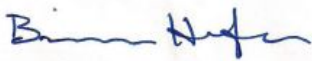
BART'S RECENT HISTORY DICTATES THAT OVERSIGHT AND TRANSPARENCY ARE REQUIRED

As described above, on April 26, 2016, the staff recommendation for the license plate reader proposal was not approved by the Board. However, the license plate readers were installed anyway, and data on BART's customers was sent to NCRIC, the San Francisco federal-state-fusion center¹. Between January and October 2017, data pertaining to 57,632 customers was sent to NCRIC, which hosts ICE agents in its headquarters, and allows ICE access to its data. As a sanctuary district, this is an egregious action and ignorance of the balance of power at BART, it may have endangered BART's undocumented riders among others, and it should never have occurred.

During our drafting of the SEO, staff asked that the BART Watch App be excluded from the SEO's coverage. Unbeknownst to me at the time, BART was in active litigation over the app's collection of certain identifying information, including unique phone identifier (IMSI or IMEI code), and location data. Although it appears that the parties have reached settlement in principal, the litigation is still active². More disheartening is that staff knew the app was a concern, was collecting invasive information, and intentionally asked to have it excluded from oversight.

It is undisputed that throughout human history, surveillance has disproportionately impacted certain communities. Whether it is the New York police department's deliberate focusing of cameras on the front doors of mosques³, creation of fake social media accounts to intentionally monitor Black Lives Matters activists like the Memphis police set up⁴, or BART's own racial disparity in its use of force⁵, it is would irresponsible of the Board to simply hand over the reins to the proposed powerful and invasive system wide mass surveillance system, without any due diligence. BART's recent history sadly demonstrates that it is not deserving of such trust.

Sincerely,



Brian Hofer
Member, Oakland Privacy
Phone: (510) 303-2871
E-Mail: contact@oaklandprivacy.org
E-Mail: brianhofer@gmail.com

¹ See attached NCRIC document.

² BART and Elerts (the vendor), have represented that the data at issue is no longer collected.

³ <https://www.ap.org/ap-in-the-news/2012/with-cameras-informants-nypd-eyed-mosques>

⁴ <https://www.theguardian.com/us-news/2018/aug/01/memphis-police-black-lives-matter-activists>

⁵ <https://www.eastbaytimes.com/2018/06/12/african-americans-involved-in-more-than-half-of-bart-use-of-force-confrontations/>