ELECTRONIC FRONTIER FOUNDATION

August 8, 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)

BART Board of Directors
300 Lakeside Drive
Oakland, CA 94604-2688

Re: Proposed face surveillance system and proposed "Physical Security Information Management System"

Dear Directors:

I am writing today on behalf of the Electronic Frontier Foundation, a non-profit member-supported civil liberties organization based in San Francisco working to protect rights in the digital world. Founded in 1990, EFF has over 40,000 dues-paying members, including thousands in California.

We encourage you to consider your own previous decisions and to reject any proposed surveillance system that fails to address established community concerns regarding transparency, privacy, oversight, and accountability. Accordingly, the Board should reject two proposals under consideration today.

Previously, the Board and its committees have discussed various provisions for transparency and public oversight.[1] Those provisions have not been met by any proposal that the Board will review today.

Among the proposals are a "Safety and Security Action Plan" that includes a provision for a "Physical Security Information Management system" (PSIM):

> The system was originally designed to monitor physical alarms and fixed sensors, but it can be enhanced to include cutting edge video analytics. A fully upgraded

[1] *See* Notice of Meeting and Agenda, BART Board Communications and Technology Modernization Committee (May 25, 2016), available at https://www.bart.gov/sites/default/files/docs/agendas/05-25-16%20BC%26TMCommittee.pdf.

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

> system would be capable of monitoring thousands of simultaneous video streams and automating response recommendation to BPD dispatch. The system automatically detects when normal patterns are disrupted, and it then sends an alert to dispatch to monitor the area. Systemwide implementation could take 12 months. Estimated cost is $4 million for implementation and $1.3 million in ongoing costs.[2]

In addition, at least one member of the Board has publicly suggested that BART consider adopting controversial and untested face surveillance technology in response to recent incidents of violent crime at BART stations.[3]

Neither of these proposals, however, address any of the parameters that Board members previously identified as crucial requirements before approving new surveillance technology.

For instance, there has been no analysis of how either PSIM or the proposed face surveillance system could impact privacy. Nor has BART analyzed how they might inhibit dissent, which is crucial given BART's previous decisions to adopt security precautions that interfered with First Amendment rights.[4]

In addition, BART has not assessed how either system could facilitate discrimination and fuel established biases marginalizing riders of color. This failure is especially perverse given the bias apparent in the gruesome crime that unfortunately prompted the premature proposals under consideration today.

The proposals also lack any accompanying use policy specifying protocols for data collection, data retention, data sharing, data security, or the purposes for which the system could be used.

Because no constraints have been discussed, we urge you to reject both the PSIM proposal and any proposed plan to adopt face surveillance, including the system proposed by Director Josefowitz. Instead, the Board should insist upon a rigorous process to assess these various risks before proceeding.

---

[2] BART General Manager proposes Safety and Security Action Plan (Aug. 6, 2018), available at http://www.bart.gov/news/articles/2018/news20180806.

[3] *See* Rachel Swan, *BART announces new safety measures in aftermath of recent violent attacks*, S.F. Chronicle (Aug. 6, 2018), available at https://www.sfchronicle.com/bayarea/article/BART-announces-new-safety-measures-in-aftermath-13135744.php.

[4] *See, e.g.*, Matt Cagle, *Five Years Later, BART's Cell Service Shutdown is Still a Wakeup Call*, ACLU of Northern Cal., (Aug. 11, 2016), available at https://www.aclunc.org/blog/five-years-later-barts-cell-service-shutdown-still-wakeup-call.

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

In particular, the high error rates associated with facial recognition technologies can physically endanger the innocent people who are then mistaken by police for wanted criminal suspects. This "false positive" risk is higher for racial minorities. The *Washington Post* recently reported that "Today's facial-recognition systems more often misidentify people of color because of a long-running data problem…."[5] That means that algorithms trained to recognize faces are both less likely to help apprehend legitimate suspects when used to identify people of color, and also more likely to enable racial profiling.

The dangers of misidentifying riders of color can hardly be overstated. Most concretely, misidentifications could easily invite state violence. BART Police have killed unarmed people before.[6]

Moreover, the mere specter of misidentification could drive a chilling effect on speech and political participation. This is no hypothetical fear: police across the Bay Area have been implicated in suppressing dissent, including through lax controls over the use of imagery placing community members at risk for both state and vigilante violence.[7]

Indeed, the FBI's recent invention of "black identity extremism" suggests a particular parade of potential horrible outcomes.[8] Communities responding to police violence have been designated by the FBI as potential threats to public safety, recalling the COINTELPRO era when civil rights organizers, including Dr. Martin Luther King, Jr., were targeted by authorities arbitrarily.[9] Dr. King's contemporary successors should not

---

[5] Drew Harwell, *Facial recognition technology is finally more accurate in identifying people of color. Could that be used against immigrants?*, Washington Post (June 28, 2018), available at https://www.washingtonpost.com/technology/2018/06/28/facial-recognition-technology-is-finally-more-accurate-identifying-people-color-could-that-be-used-against-immigrants/.

[6] *See* Alyssa Jeong Perry, *Nine Years After Oscar Grant's Death, His Mother Continues to Speak Out*, KQED (January 1, 2018) available at https://www.kqed.org/news/11639679/nine-years-after-oscar-grants-death-his-mother-continues-to-speak-out.

[7] *See* Sam Levin, *Berkeley police under fire for publishing anti-fascist activists' names and photos*, The Guardian (Aug. 6, 2018), available at https://www.theguardian.com/us-news/2018/aug/06/berkeley-activists-arrested-police-identified-twitter.

[8] *See* Khaled A. Beydoun & Justin Hansford, *The F.B.I.'s Dangerous Crackdown on 'Black Identity Extremists'*, Washington Post (Nov. 15, 2017), available at https://www.nytimes.com/2017/11/15/opinion/black-identity-extremism-fbi-trump.html (noting that "This designation, just recently invented by the F.B.I., is as frightening and dangerous as the bureau's infamous Cointelpro program of the 1960s and '70s, under which J. Edgar Hoover set out to disrupt and destroy virtually any group with the word 'black' in its name.").

[9] See Dia Kayyali, *FBI's "Suicide Letter" to Dr. Martin Luther King, Jr., and the Dangers of Unchecked Surveillance*, EFF (Nov. 12, 2014), available at

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

have to fear their regional transit system fueling federal efforts to target them based on their political speech.

Short of suppressing political speech, face surveillance could also be used to track riders' locations and compile detailed historical dossiers of their movements. This information can be incredibly revealing, as the Supreme Court recently recognized when requiring a judicial warrant for authorities to access historical cell-site location information from private telecom firms.[10]

Finally, new surveillance technologies, like the ones at issue here, pose a threat to the Bay Area's immigrant communities. These spying systems will generate a massive amount of sensitive information about the comings and goings of vast numbers of travelers. If federal immigration officials obtain access to it, as they have from other state and local governments, it could be used to locate and deport undocumented workers and students.

Ultimately, the parameters and protocols of a potential facial recognition system have been neither disclosed, nor debated. Before approving such an expansion of surveillance, the Board should be fully informed. At the very least, a privacy impact statement should be prepared and subjected to public review, as well as a policy specifying the protocols and parameters for its use.

The Board should consider any proposed surveillance measure only after completing a rigorous and open process to identify the potential risks to privacy, dissent, immigrants, and communities of color. If the Board decides that the benefits outweigh the costs, it should ensure the adoption of an appropriate privacy policy constraining the use of any such system. This approach maximizes opportunities to protect the rights of riders, encourages legitimacy by allowing community participation, and ensures the Board's effective control over law enforcement.

Please do not hesitate to contact me to discuss any questions you may have. I can be reached by email at shahid@eff.org or by phone at 415-436-9333 ext. 171.

Sincerely,

Shahid Buttar
Director of Grassroots Advocacy

---

https://www.eff.org/deeplinks/2014/11/fbis-suicide-letter-dr-martin-luther-king-jr-and-dangers-unchecked-surveillance.

[10] *See* U.S. v. Carpenter, 585 U.S. ___ (2018) (requiring a judicial warrant before law enforcement may access cell-site location information from telecom providers).

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org