ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

February 11, 2016

Santa Clara Board of Supervisors
Finance and Government Operations Committee
70 West Hedding Street
10th Floor, East Wing
San Jose, CA 95110

Dear Committee members:

I write today to express support for the Surveillance-Technology and Community-Safety ordinance on behalf of the Electronic Frontier Foundation (EFF), a non-profit member-supported civil liberties organization based in San Francisco working to protect rights in the digital world. EFF represents more than 25,000 dues-paying members and supporters across the country.

The proposed ordinance addresses an increasing need for transparency and oversight of law enforcement and public safety activities that can—if left to proceed unfettered—easily undermine civil liberties and civil rights.

We urge you to forward the proposal to the Board of Supervisors with a favorable recommendation, with a few caveats.

In particular, we write to offer two suggestions for potential amendments, highlight one important component of the proposed ordinance, and present a local story from within your jurisdiction about how law enforcement surveillance can impact the lives of real people.

A case study from San Jose

A story our organization recently uncovered helps illustrate how the lives of your constituents can be impacted by surveillance when used without adequate safeguards.

Last year, EFF obtained through the California Public Records Act a copy of the San Jose Police Department's revised 2012 Annual Report on its participation in the Santa Clara County's CAL-ID program. In the document, SJPD discussed a facial recognition pilot program and cited a case example of how they were able to use the technology to identify a violent crime suspect and issue an arrest warrant.

EFF took a deeper look at the purported success story. After pulling the case file and interviewing the defense attorney, we learned that the case was ultimately dropped when it became clear that SJPD arrested the wrong young man. We also learned

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

that the use of experimental facial recognition technology was never disclosed to the defendant's attorney; officers only said they ran the photo through a database.

SJPD did not provide us with usage policies for facial recognition. We further asked SJPD to provide us with the facial recognition access log associated with the case. The city told us they could not, since when the pilot project ended, they no longer had access to the records. When we asked for statistical data on arrests that were assisted by facial recognition, we were again told there was no data.

SJPD portrayed this case as a success, when what it actually demonstrated was the danger of giving law enforcement high-tech tools without adequate transparency, oversight, and review.

In 2015, years after the pilot ended, SJPD applied for a federal grant to build a more permanent, county-wide facial recognition system. They did not receive it, but SJPD told us they were pursuing other funding options.

This episode should serve as a warning.

Suggested amendments

We propose two amendments to clarify, focus, and strengthen the proposal.

First, we suggest revisions to the definition of "Surveillance technology" in Section 7(C). In particular, we propose amending Section 7(c) as follows:

> "Surveillance technology" means any electronic device, system using an electronic device, or similar technological tool used, designed, or primarily intended to collect, retain, process, or share audio, communications, visual, location, thermal, olfactory, biometric or similar information specifically associated with, or capable of being associated with, any individual or group, without the express consent of that individual or group. Presence in a public area, alone, may not constitute such consent.
>
> ~~Examples of~~ Surveillance technology includes, but is not limited to, drones with cameras or monitoring capabilities, automated license plate readers, closed-circuit cameras/televisions, cell-site simulators, International Mobile Subscriber Identity (IMSI) trackers, Global Positioning System (GPS) tracking technology, radio-frequency identification (RFID) technology, audio detection devices such as ShotSpotter, rapid DNA collection tools, iris scanners, and facial-recognition technology.

Including "communications" information among the kinds of information that, if collected, render the object of collection a method of "surveillance technology" will ensure that the ordinance encompasses the various methods used to collect

telecommunications content and metadata. Including "biometric" will ensure the ordinance encompasses software and tools used to identify people using their biometric information like iris scans, face recognition, and DNA. Many of these tools are now or will be in the near future capable of identifying people at a distance, without their knowledge or consent.

Meanwhile, including the caveat regarding the express consent of individuals monitored is important to exclude from the proposed definition the variety of devices purchased by county agencies that store information but are not used to monitor members of the public. Finally, we suggest making the default rule favor your constituents by making explicit that being present in a public area does not express consent to be monitored or subjected to surveillance.

Second, we suggest mandating a simple process through which agencies can certify as exempt from the ordinance's requirements devices from which data will not be shared with or routinely accessible by law enforcement agencies. A measure along these lines will focus the ordinance's reporting requirements on devices used to conduct surveillance and avoid squandering resources on assessing recording devices used for other purposes. Specifically, we suggest amending the ordinance to provide that:

> Civil agencies not involved in law enforcement or code enforcement may exempt particular information-recording devices and systems from the requirements applied to "surveillance technology" by certifying that data from those devices or systems will not be accessible by law enforcement agencies absent exigent circumstances.

This formulation will require the registration of devices, without burdening the oversight process. To the extent any particular use of certified devices or systems later grows controversial, the registration of the devices will enable journalists and constituents to leverage CPRA to investigate.

Finally, we particularly praise the proposal's recognition of a pattern and practice among law enforcement departments to seek forgiveness rather than permission, by applying the process and reporting requirements to *all* uses of technology for surveillance purposes, rather than a specific device.

The State of California became a national leader in 2015 by regulating particular surveillance methods, specifically IMSI-catchers and Automated License Plate Reader systems, that had already been widely used by agencies across the state for nearly a decade. Your constituents should not need to wait for years before securing the public transparency your community deserves.

Respectfully submitted,

Shahid Buttar
Electronic Frontier
Foundation