March 30, 2022

VIA ELECTRONIC MAIL
Committee on Information Technology
City Hall, Room 352
1 Dr. Carlton B. Goodlett Place
San Francisco, CA 94102
coit.staff@sfgov.org

Re: Opposition to SFPD Surveillance Technology Policy on Non-City Entity Surveillance Cameras

Dear Committee on Information Technology ("COIT") Members:

The Electronic Frontier Foundation ("EFF")[1] and the ACLU of Northern California ("ACLU NorCal")[2] respectfully oppose the San Francisco Police Department's ("SFPD") draft Surveillance Technology Policy governing Non-City Entity Surveillance Cameras ("the Policy").[3] The Policy drastically expands the SFPD's power to access non-city surveillance cameras—including cameras owned by private businesses, organizations, and even residents—and allows the SFPD to use these cameras for unprecedented live monitoring. The Policy proposes a seismic shift from police relying on non-city cameras for historical footage in specific situations, to authorizing the use of live monitoring in a broad range of circumstances. The Policy is also vague, failing to define key terms and failing to adequately explain when the SFPD can and cannot use non-city cameras. We urge COIT to reject the Policy and start anew to carefully draft a policy that protects San Franciscans' privacy and civil liberties.

Our foremost concern is that the Policy allows the SFPD to engage in unprecedented and programmatic live monitoring of privately-owned cameras in a broad range of circumstances. The Policy authorizes, among other uses, "[t]emporary live monitoring

[1] EFF is a member-supported, nonprofit civil liberties organization that protects free speech and privacy rights in the digital world. EFF was founded in 1990, is headquartered in San Francisco, and has more than 35,000 members.
[2] ACLU NorCal is a non-profit, non-partisan civil liberties organization and a California affiliate of the national American Civil Liberties Union. ACLU NorCal was founded in 1934 and today has more than 100,000 members dedicated to the principles of liberty and equality embodied in both the United States and California constitutions.
[3] *Available at https://sf.gov/sites/default/files/2022-03/SFPD%20Non%20City%20Entity%20Surveillance%20Camera%20STP_Draft-UPDATE%20for%203.31.22%20PSAB%20review.pdf.*

during active criminal investigations and significant events with public safety concerns."[4] Notably, the Policy does not define "active criminal investigations" or "significant events with public safety concerns." The Policy also authorizes the SFPD to live monitor "large-scale events" or in "areas in [the] city that pose security risks to visitors and residents,"[5] and again, defines neither. This vagueness may reduce limits on when and where the SFPD may conduct live monitoring, and provides little guidance to officers and the public alike about the SFPD's use of these cameras. People should be able to live in, walk around, and work in San Francisco without the fear that police are watching them as they go about their daily lives.

The Policy's prohibition on surveillance of activity protected by the First Amendment is similarly vague and risks authorizing the SFPD to spy on protesters and other people who speak out on social and political issues. The Policy prohibits the SFPD from accessing live camera feeds during First Amendment-protected activities, except to assess "redeployment needs due to crowd sizes" or "other issues creating public safety hazards."[6] Again, the Policy defines neither term. This vague and broad phrasing risks allowing the SFPD to live monitor any event where people congregate, including protests and other civic gatherings.

Even the advocates of most non-city cameras never intended them for live police surveillance, particularly the camera networks run by community benefit districts ("CBDs") and business improvement districts ("BIDs") across the city. Chris Larsen, a financial backer of CBD/BID camera networks, has publicly stated that law enforcement is prohibited from using the networks for live surveillance.[7] The executive director of the Tenderloin CBD, Simon Bertrang, similarly stated that "his group worked with locals to ensure the network is not real-time surveillance."[8] Thus, when community members weighed in on CBD/BID proposals to install surveillance cameras in these neighborhoods, they did not have the opportunity to discuss live police surveillance.[9] The SFPD's Policy is at odds with settled expectations about these camera networks.

---

[4] *Id.* at 1.
[5] *Id.* at 3.
[6] *Id.* at 2.
[7] Daniel Moattar, *SF Tech Moguls Funded the Cameras. Cops Used Them to Spy on Protesters.*, Mother Jones (Oct. 7, 2020), https://www.motherjones.com/anti-racism-police-protest/2020/10/sf-tech-moguls-funded-the-cameras-cops-used-them-to-spy-on-protesters/.
[8] Carolyn Said, *Crypto mogul who installed cameras in S.F. is focused on solving local, global problems*, S.F. Chronicle (Sept. 27, 2021), https://www.sfchronicle.com/tech/article/Crypto-mogul-who-installed-cameras-in-S-F-is-16486005.php.
[9] Nellie Bowles, *Why Is a Tech Executive Installing Security Cameras Around San Francisco?*, N.Y. Times (July 10, 2020), https://www.nytimes.com/2020/07/10/business/camera-surveillance-san-francisco.html (quoting Tenderloin CBD executive director Bertrang to explain why some preferred to establish camera networks through CBDs/BIDs: "If you went to the board of supervisors and asked the members to approve this, you'd end up having a conversation about government and surveillance.").

In addition, the Policy even permits the SFPD to seek live viewing access to a wide array of cameras in both public and private spaces. The Policy's definition of non-city entity surveillance cameras includes those in residential, small business, and commercial security spaces, and for both indoor and outdoor use.[10] The Policy also includes smart and doorbell cameras "affixed to or inside of a residence"[11] within its definition. Thus, this broad definition includes cameras used by businesses (which are traditionally considered to be non-city entity surveillance cameras) *and* private residential cameras (which are traditionally not). While some San Francisco homeowners and renters may expect the SFPD to request historical footage caught by cameras on their properties, they do not expect the SFPD to use their cameras for real-time surveillance.

Altogether, the Policy would permit the SFPD to make frequent and sweeping requests for live viewing access through privately-owned cameras. While a non-city actor "retains the right" to say no to the SFPD's requests for live access,[12] many people, especially marginalized people, will feel immense pressure to give in to the SFPD. This will inevitably lead to police officers viewing residential and business surveillance cameras in real-time, including nearby or inside of sensitive and private locations such as clinics, places of worship, and homes.

COIT must reject the SFPD's attempted overreach, particularly because there are existing, narrowly defined circumstances under which the SFPD can use non-city cameras for live monitoring: in "an emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use" of the technology.[13] Such exigent circumstances would allow the SFPD to use non-city cameras in a targeted manner when necessary to prevent harm to a person while also respecting privacy and civil liberties.

The Policy's provisions on SFPD access to historical footage recorded by non-city cameras also significantly threatens San Franciscans' civil liberties and civil rights.

First, the Policy authorizes "[r]eviewing specific historical footage to aid a criminal or internal investigation."[14] Again, it does not define those terms, and fails to provide guidance to officers and the public alike about when the SFPD may seek such footage. This is important because, in at least one incident, the SFPD previously requested and received a "data dump" of 12 hours of footage from all cameras in the Union Square BID

[10] *Supra* n.3 at 2-3.
[11] *Id.* at 3.
[12] *Id.* at 5.
[13] S.F. Admin. Code §§ 19B.7, 19B.1.
[14] *Supra* n.3 at 2.

during racial justice protests, without identifying a specific crime under investigation.[15] The Policy must prohibit the use of non-city cameras for such fishing expeditions.

Second, the Policy allows the SFPD to retain personally identifying information from historical footage for two years,[16] raising the risk that such information will be misused or exposed in an accidental breach.

Third, the Policy relies on self-reporting by SFPD officers rather than independent auditing. The Policy requires officers to keep a chronological file of their requests for surveillance footage and associated details. The Policy claims this will "serve as the Department's audit log."[17] Self-reporting is insufficient to prevent unauthorized access. This is especially a problem because virtually anyone at the SFPD, ranging from non-sworn members to the chief of police, may request historical footage.[18]

For all of these reasons, EFF and ACLU NorCal respectfully urge COIT to reject the SFPD's proposed Policy and start anew to draft a policy that respects the privacy and civil liberties of San Franciscans. If you have any questions or concerns, please contact Saira Hussain at saira@eff.org (415) 436-9333 ext. 204.

Sincerely,

Saira Hussain
Staff Attorney
Electronic Frontier Foundation

Matt Cagle
Staff Attorney
ACLU of Northern California

CC: Jillian Johnson, COIT Director
Linda Gerull, Executive Director of the Department of Technology
Carmen Chu, City Administrator
Angela Calvillo, Clerk of the Board
Michael Makstman, City Chief Information Security Officer
Bill Scott, Chief of Police

[15] Dave Maass & Matthew Guariglia, *San Francisco Police Accessed Business District Camera Network to Spy on Protestors*, EFF Deeplinks (July 27, 2020), https://www.eff.org/deeplinks/2020/07/san-francisco-police-accessed-business-district-camera-network-spy-protestors.
[16] *Supra* n.3 at 8-9.
[17] *Id.* at 7.
[18] *Id.* at 5.