From: Seattle Community Surveillance Working Group
(CSWG) To: Seattle City Council
Date: April 23, 2019
Re: Privacy and Civil Liberties Impact Assessment for ~~Emergency Scene Cameras, Hazardous Materials Cameras~~, SDOT CCTVs
**SFD Cameras Impact Assessments Removed by Central Staff.

Executive Summary and Background

On February 27th, CSWG received the Surveillance Impact Reports, or SIRs, for the above-mentioned technologies included in Group 1 of the Seattle Surveillance Ordinance technology review process. This document is CSWG's Privacy and Civil Liberties Impact Assessment for those technologies as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Councils.

Our assessment of these surveillance technologies focuses on three key issues:

(1) The use of these systems and the data collected by them for purposes other than those intended;
(2) Over-collection and over-retention of data;
(3) Sharing of that data with third parties (such as federal law enforcement agencies).

While the stated purposes of the cameras may be relatively innocuous, it is important to remember that images taken by such cameras, for example at emergency scenes, can compromise the privacy of individuals at vulnerable moments, and can be misused to target and profile communities based on their religious, ethnic, or associational makeup. In addition, with the widespread and inexpensive availability of facial recognition (or face surveillance) technology, which can be applied after the fact to any image showing a face, it is even more important that protections limiting the use of these tools to their intended purpose be enacted.

For all of these systems, the Council should adopt, via ordinance, clear and enforceable rules that ensure, at a minimum, the following:

1. The purposes of camera use should be clearly defined, and its operation and data collected should be explicitly restricted to those purposes only.
2. Data retention should be limited to the time needed to effectuate the purpose defined.
3. Data sharing with third parties should be limited to those held to the same restrictions.
4. Clear policies should govern operation, and all operators of the cameras should be trained in those policies.

We recommend creating these rules in a single, blanket ordinance that will govern not only these, but other, similar camera technologies operated by or at the behest of the City, and would be happy to work with the City to create such an ordinance.

1. Closed Circuit Television "Traffic Cameras" (CCTVs)(SDOT)

As with ESCs and Hazmat Cameras, concern around these traffic cameras relates to limiting their use to specific purposes, ensuring protections against invasion of privacy and general data collection, and limiting data sharing with third parties. It is important for these limits to be set forth in clear, enforceable policies. The updated January 2019 SIR states that SDOT "has developed" policies on use of the cameras, but it is not clear where all of these policies are set forth and whether they are currently in effect (see Section 3.3). We have reviewed the Camera Control Protocol document that sets forth

existing policies.

For CCTVs, the Council's approval of this technology should ensure use is limited to traffic operations, that no data is collected except for clearly specified exceptions (and that data must be deleted immediately upon completion of those purposes), and that data sharing with third parties is prohibited. More specific recommendations for the Council's approval of this technology are below.

The existing policy:

- Does not set forth clear use, collection, and retention rules.
    - *Recommendation: SDOT's adopted policy should make clear that no data may be recorded or retained except for specifically defined purposes. Currently, the SDOT Camera Control Protocol states that recording is allowed for "compelling SDOT traffic operations and traffic planning needs"—but that term is undefined. The retention of data for "engineering studies" must also be clearly defined. No personally-identifiable information should ever be recorded. For any data recording that is allowed, it must be deleted within 10 days (which is stated in the SIR and protocol) and not shared with third parties. The policy should also make clear that traffic camera data (beyond what is made available to the general public) may not be used for law enforcement purposes, and that no associated surveillance technologies such as facial recognition or license plate readers may be incorporated into the cameras.*
- Does not ensure all operators of the cameras are trained in the foregoing policies.
    - *Recommendation: This requirement should be part of any new policy.*
- Does not state include technical controls.
    - *Recommendation: Technical controls ensure logging how cameras are moved from their preset locations, when camera streams to the public are stopped or restarted, and whether there are access controls determining who, when, where, and why users can access the camera management software. Without these technical controls, it would be difficult to detect if users are abusing their access to cameras (e.g., by cutting camera feeds to the public, moving a camera to zoom and view into the window of a home). These technical controls (logging when cameras are moved, stopped, or restarted; and mandating access controls for cameras) should be included in SDOT's adopted policy.*