An Act To Promote Transparency and Protect Civil Rights and Civil Liberties With Respect to Surveillance Technology

WHEREAS, the City Council finds it is essential to have an informed public debate as early as possible about decisions related to surveillance technology.

WHEREAS, the City Council finds that no decisions relating to surveillance technology should occur without strong consideration being given to the impact such technologies may have on civil rights and civil liberties, including those rights guaranteed by the First, Fourth, and Fourteenth Amendments to the United States Constitution.

WHEREAS, t

(3) Using new or existing surveill

(a) What legal and procedural rules will govern each authorized use;

(b) What potential uses of the surveillance technology will be expressly prohibited, such as the warrantless surveillance of public events and gatherings; and

(c) How and under what circumstances will surveillance data that was collected, captured, recorded, or intercepted by the surveillance technology be analyzed and reviewed.

(3) Data Collection:

(a) What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology;

(b) What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data; and

(c) How inadvertently collected surveillance data will be expeditiously identified and deleted.

(4) Data Protection: What safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms.

(5) Data Retention: Insofar as the privacy of the public can be severely compromised by the long-term storage of mass surveillance data, what rules and procedures will govern the retention of surveillance data, including those governing:

(a) For what limited time period, if any, surveillance data will be retained. Such information shall include a statement explaining why the designated retention period is no greater than that which is absolutely necessary to achieve the specific purpose(s) enumerated in the Surveillance Use Policy;

(b) What specific conditions must be met to retain surveillance data beyond the retention period stated in Section 2(C)(5)(a);

(c) By what process surveillance data will be regularly deleted after the retention period stated in Section 2(C)(5)(a) elapses and what auditing procedures will be implemented to ensure data is not improperly retained;

(6) Surveillance Data Sharing: If a municipal entity is seeking authorization to share access to surveillance technology or surveillance data with any other governmental agencies, departments, bureaus, divisions, or units, it shall detail:

(a) How it will require that the collection, retention, and storage of surveillance data be conducted in compliance with the principles set forth in 28 C.F.R. Part 23, including by not limited to 28 C.F.R. Part 23.20(a), which states that a government entity operating a surveillance program “shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.”

(b) Which governmental agencies, departments, bureaus, divisions, or units will be approved for (i) surveillance technology sharing, and for (ii) surveillance data sharing;

(c) How such sharing is necessary for the stated purpose and use of the surveillance technology;

(d) How it will ensure any entity sharing access to the surveillance technology or surveillance data complies with the applicable Surveillance Use Policy and does not further disclose the surveillance data to unauthorized persons and entities; and

(e) What processes will be used to seek approval of future surveillance technology or surveillance data sharing agreements from the municipal entity and City Council.

(7) Demands for Access to Surveillance Data: What legal standard must be met by government

(8) Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Use

on any community or group. To assist the public in participating in such an analysis, all approved Surveillance Impacts Reports and Surveillance Use Policies shall be made available to the public, at a

(B) Within thirty (30) days of submitting and publicly releasing an Annual Surveillance Report pursuant to Section 6(A), the municipal agency shall hold one or more well-publicized and conveniently located community engagement meetings at which the general public is invited to discuss and ask questions regarding the Annual Surveillance Report and the municipal agency's use of surveillance technologies.

(C) Based upon information provided in the Annual Surveillance Report, the City Council shall determine whether each surveillance technology identified in response to Section 6(A), as used by the report-submitting entity, has met the standard for approval set forth in Section 4. If it has not, the City Council shall direct the

(E)

(C) “Municipal entity” shall mean any municipal government, agency, department, bureau, division, or unit of this City.

(D) “Surveillance data” shall mean any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by surveillance technology.

(E) “Surveillance technology” shall mean any electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.

(1) “Surveillance technology” includes, but is not limited to: (a) international mobile subscriber identity (IMSI) catchers and other cell site simulators; (b) automatic license plate readers; (c) electronic toll readers; (d) closed-circuit television cameras; (e) biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases; (f) mobile DNA capture technology; (g) gunshot detection and location hardware and services; (h) x-ray vans; (i) video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; (j) surveillance enabled or capable lightbulbs or light fixtures; (k) tools, including software and hardware, used to gain unauthorized access to a computer, computer ser

(F) “Viewpoint-based” shall mean targeted at any community or group or its members because of their exercise of rights protected under the First Amendment of the United States Constitution.

Section 13. Severability

The provisions in this Act are severable. If any part of provision of this Act, or the application of this Ae