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

Findings

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

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 individual rights and liberties, including the right to privacy..

The City Council finds that legally enforceable safeguards, including robust transparency, oversight, and accountability measures, must be in place to protect individual rights and liberties before any surveillance technology is deployed.

The City Council finds that, if a surveillance technology is approved, data reporting measures must be adopted that empower the City Council and public to verify that mandated individual rights and liberties safeguards have been strictly adhered to.

The City Council finds that the full cost of a surveillance technology should be considered and made publically available to analyze if its financial benefits outweigh its costs and if an expenditure on such a technology is in the best interest of the City.

NOW, THEREFORE, BE IT RESOLVED that the City Council adopts the following:

Section 1

For the purposes of this Act:

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

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

(C) “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 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 service, or computer network; (l) social media monitoring software; (m) through-the-wall radar or similar imaging technology, (n) passive scanners of radio networks, (o) long-range Bluetooth and other wireless-scanning devices, (p) radio-frequency I.D. (RFID) scanners, and (q) software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software. The enumeration of surveillance technology examples in this subsection shall not be interpreted as an endorsement or approval of their use by any municipal entity.

(2) “Surveillance technology” does not include the following devices or hardware, unless they have been equipped with, or are modified to become or include, a surveillance technology as defined in Section 1(E): (a) routine office hardware, such as televisions, computers, and printers, that is in widespread public use and will not be used for any surveillance or law enforcement functions; (b) Parking Ticket Devices (PTDs); © manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) municipal agency databases that do not and will not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology; and (f) manually-operated technological devices that are used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems.

Section 2

(A) A municipal entity must obtain City Council approval, subsequent to a mandatory, properly noticed, germane, public City Council hearing at which the public is afforded a fair and adequate opportunity to provide written and oral testimony, prior to engaging in any of the following:

(1) Seeking funds for new surveillance technology, including but not limited to applying for a grant, or soliciting or accepting state or federal funds or in-kind or other donations;

(2) Acquiring or borrowing new surveillance technology, whether or not that acquisition is

made through the exchange of monies or other consideration;

(3) Using new or existing surveillance technology for a purpose or in a manner not previously approved by the City Council in accordance with this Act; or

(4) Soliciting proposals for or entering into an agreement with any other person or entity to acquire, share or otherwise use surveillance technology or surveillance data.

(B) Prior to seeking approval pursuant to Section 2(A) for the funding, acquisition, or use of surveillance technology or the entry into an agreement concerning such funding, acquisition, or use, a municipal entity shall submit to the City Council a Surveillance Impact Report and Surveillance Use Policy concerning the technology at issue at least forty-five (45) days prior to the public hearing.

(1) The City Council shall publicly release, in print and online, the Surveillance Impact Report and Surveillance Use Policy at least thirty (30) days prior to the public hearing.

(2) The City Council, or its appointed designee, shall continue to make the Surveillance Impact Report and Surveillance Use Policy, and updated versions thereof, available to the public as long as the municipal entity continues to utilize the surveillance technology in accordance with its request pursuant to Section 2(A).

(C) No use of surveillance technology by a municipal entity pursuant to Section 2(A) shall be permitted without the City Council's express approval of the related Surveillance Impact Report and Surveillance Use Policy submitted by the municipal entity pursuant to Section 2(B).

(D) Prior to approving or rejecting a Surveillance Impact Report or Surveillance Use Policy, the City Council may request revisions be made by the submitting municipal entity. Revisions should be requested where any inadequacies are perceived to exist within a Surveillance Use Policy or Surveillance Impact Report.

(1) Any requested revisions to a Surveillance Impact Report or Surveillance Use Policy made by a member, employee, or committee of the City Council, and the responses thereto, shall be publicly released by the City Council, in print and online, at least thirty (30) days prior to any City Council vote to approve or reject a request made by a municipal entity pursuant to Section 2(A).

(2) In the event revisions are made to the originally submitted Surveillance Impact Report or Surveillance Use Policy, prior to voting to approve or reject the revised Surveillance Impact Report or Surveillance Use Policy, the City Council shall hold another properly noticed, germane, public City Council hearing at which the public is afforded a fair and adequate opportunity to provide written and oral testimony on the

revised Surveillance Impact Report and/or Surveillance Use Policy. A copy of the revised Surveillance Impact Report and/or Surveillance Use Policy shall be publicly released by the City Council, in print and online, at least thirty (30) days prior to such a public hearing.

(E) A Surveillance Impact Report submitted pursuant to Section 2(B) shall be a publicly released, legally enforceable written report that includes, at a minimum, the following:

(1) Information describing the surveillance technology and how it works, including product descriptions from manufacturers;

(2) Information on the proposed purpose(s) for the surveillance technology;

(3) If the surveillance technology will not be uniformly deployed or targeted throughout the City:

(a) What factors will be used to determine where the technology is deployed or targeted; and

(b) Based upon those factors enumerated pursuant to Section 2(E)(3)(a), what geographical location(s) are anticipated to receive a disproportionally high level of deployment or targeting;

(4) The fiscal impact of the surveillance technology, including but not limited to:

(a) Initial acquisition costs;

(b) Ongoing operational costs such as personnel, legal compliance, use auditing, data retention and security costs;

(c) Any cost savings that would be achieved through the use of the technology; and

(d) Any current or potential sources of funding; and

(5) An assessment identifying with specificity:

(a) Any potential impacts the surveillance technology, if deployed, might have on individual liberties and rights, including but not limited to:

(i) Potential adverse impacts on privacy and anonymity rights;

(ii) Potential adverse impacts on the individual rights and liberties guaranteed by the First and Fourth, Amendments to the United States Constitution and [relevant sections from the state constitution's bill of rights]; and

(b) What specific, affirmative measures will be implemented to safeguard the public from each of the potential disparate and adverse impacts identified pursuant to Section 2(E)(5)(a).

(6) A disclaimer that the Surveillance Impact Report shall be considered a draft proposal until such time as it is approved, with or without modifications, pursuant to a vote of the City Council.

(F) A Surveillance Use Policy submitted pursuant to Section 2(B) shall be a publicly-released, legally enforceable written policy governing the municipal entity's use of the surveillance technology that, at a minimum, includes and addresses the following:

(1) Purpose: What specific purpose(s) that the surveillance technology is intended to advance.

(2) Authorized Use: What specific surveillance technology use(s) is authorization being sought for, and:

(a) Whether the surveillance technology will be operated continuously or used only under specific circumstances;

(b) Whether the surveillance technology will be installed permanently or temporarily;

(c) Whether the surveillance technology will be uniformly deployed or targeted throughout the city, and, if not, what factors will be used to determine where the technology is deployed or targeted;

(d) What rules will govern, and what processes will be required prior to each use of the surveillance technology, including but not limited to:

(i) For each authorized use enumerated pursuant to Section 2(F)(2):

a. What existing legal standard must be met before the technology is used, or, where such a standard does not currently exist, what is the proposed standard to be followed;

b. Whether a judicial warrant is required; and

c. What information must be included in any warrant or court authorization granting permission to use the device;

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

(f) The extent to which, and how the surveillance technology will be used to monitor persons in real time, as data is being captured;

(g) Whether the surveillance technology will be used to investigate (i) violent crimes, (ii) non-violent crimes, (iii) felonies, (iv) misdemeanors, and (v) other legal violations and/or infractions not classified as felonies or misdemeanors; and

(h) The extent to which, how, and under what circumstances retained surveillance data that was collected, captured, recorded, or intercepted by the surveillance technology will be analyzed or reviewed.

(3) Data Collection:

(a) What types of surveillance data are capable of being 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, consistent with Section 2(F)(7)(f), inadvertently collected data identified in Section 2(F)(3)(b) will be expeditiously identified and deleted.

(4) Database Reliance: Where applicable, what databases will the technology rely upon to make subject identifications.

(5) Data Access:

(a) Under what circumstances will an individual will be allowed to request access to surveillance data, who will be responsible for authorizing access to the surveillance data, what rules and processes must be followed prior to accessing or interacting with the surveillance data, and what are the acceptable grounds for requesting access to the surveillance data;

(b) What type of viewer’s log or other comparable method will be used to track viewings of any surveillance data and what information will it track;

(c) A description of what individuals will have the authority to obtain copies of the surveillance data and what procedures will be put in place to prevent the unauthorized distribution of the copied surveillance data.

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

(7) Data Retention: What rules and procedures will govern the retention of surveillance data, including those governing:

(a) For what time period, if any, surveillance data will be retained. Such information shall include a statement as to why the designated retention period is appropriate in light of the 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(F)(7)(a);

(c) By what process will surveillance data be regularly deleted after the retention period stated in Section 2(F)(7)(a) elapses and what auditing procedures will be implemented to ensure data is not improperly retained beyond the retention period;

(d) What methods will be used to store surveillance data, including how will the surveillance data is to be labeled or indexed;

(e) What methods will be used to identify surveillance data that has been improperly collected and/or retained, and how will that data, including any copies thereof, be expeditiously destroyed once it is identified;

(f) What process will be put into place so individuals who claim surveillance data pertaining to them has been improperly collected and/or retained can petition to have their claims reviewed and how will improperly collected or retained surveillance data, including any copies thereof, be expeditiously destroyed once it is identified;

(g) What technological system will be used to store the surveillance data, and who will maintain custody and control over the system and its surveillance data; and

(h) What unit or individuals will be responsible for ensuring compliance with Section 2(F)(7), and when and how compliance audits will be conducted.

(8) Public Access: How will surveillance data be accessible to members of the public, how does the municipal entity interpret the applicability of, and intend to comply with [insert name of applicable public records act(s)], and what steps will be taken to protect individual privacy.

(9) Target/Defendant Access: How, to what extent, and when will surveillance data, in accordance with applicable law, be accessible to targets of criminal or civil investigations, criminal or civil defendants, and their attorneys.

(10) Surveillance Data Sharing: If a municipal entity intends 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.
>
> (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 required 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.

(11) Demands for Access to Surveillance Data: What legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.

(12) Training: What training, including training materials, will be required for any individual authorized to use the surveillance technology or to access surveillance data.

(13) Maintenance: How will the security and integrity of the surveillance technology be maintained and how the will the municipal entity or lead agent present any substantive changes in the surveillance technology's functionality to the City Council for approval.

(14) Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Use Policy is followed, including what internal personnel will be assigned to ensure compliance with the policy, what independent persons or entities will be given oversight authority, and what legally enforceable sanctions will be put in place for violations of the policy.

(15) Complaints: What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific surveillance technology, and what internal personnel will be assigned to receive, register, track, and respond to such communications.

(16) The Surveillance Use Policy shall include a disclaimer that the Surveillance Use Policy shall be considered a draft proposal until such time as it is approved, with or without modifications, pursuant to a vote of the City Council.

Section 3

No later than one hundred twenty (120) days following the effective date of this Act, any municipal entity seeking to continue the use of any surveillance technology it was in use prior to the effective date of this Act must commence a City Council approval process in accordance with Section 2(A)(3). If the City Council has not approved the continuing use of the surveillance technology, including the Surveillance Impact Report and Surveillance Use Policy re submitted pursuant to Section 2(B), within one hundred eighty (180) days of their submission to the City Council, the municipal entity shall cease its use of the surveillance technology until such time as City Council approval is obtained in accordance with this Act.

Section 4

If more than one municipal entity will have access to the surveillance technology or surveillance data, a lead municipal entity shall be identified. The lead municipal entity shall be responsible for maintaining the surveillance technology and ensuring compliance with all related laws, regulations and protocols. If the lead municipal entity intends to delegate any related responsibilities to other governmental agencies, departments, bureaus, divisions, units, or personnel, these responsibilities and associated entities and/or personnel shall be clearly identified.

Section 5

The City Council shall only approve a request to fund, acquire, or use a surveillance technology if it determines the benefits of the surveillance technology outweigh its costs, and that the proposal will safeguard individual liberties and rights. 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 designated page on the relevant municipal entity’s public

website, for as long as the related surveillance technology remains in use. An approval for the funding, acquisition and/or use of a surveillance technology by the City Council, where the risk of potential adverse impacts on individual rights or liberties have been identified in the Surveillance Impact Report pursuant to Section 2(D)(5)(a), shall not be interpreted as an acquiescence to such impacts, but rather as an acknowledgement that a risk of such impacts exists and must be proactively avoided.

Section 6

(A) A municipal entity that obtains approval for the use of surveillance technology must submit to the City Council an Annual Surveillance Report for each specific surveillance technology used by the municipal entity within twelve (12) months of City Council approval, and annually thereafter on or before March 15. The Annual Surveillance Report shall, at a minimum, include the following information for the previous calendar year:

(1) A summary of how the surveillance technology was used;

(2) Whether and how often collected surveillance data was shared with any external persons or entities, the name(s) of any recipient person or entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

(3) Where applicable, a breakdown of where the surveillance technology was deployed geographically, by individual census tract as defined in the relevant year by the United States Census Bureau. For each census tract, the municipal entity shall report how many individual days the surveillance technology was deployed and what percentage of those daily-reported deployments were subject to (A) a warrant, and (B) a non-warrant form of court authorization;

(4) Where applicable, a breakdown of how many times the surveillance technology was used to investigate potential or actual (A) violent crimes, (B) non-violent crimes, (C) felonies, (D) misdemeanors, and (E) other legal violations and/or infractions not classified as felonies or misdemeanors

(5) Where applicable, and with the greatest precision that is reasonably practicable, the amount of time the surveillance technology was used to monitor Internet activity, including but not limited to social media accounts, the number of people affected, and what percentage of the reported monitoring was subject to (A) a warrant, and (B) a non-warrant form of court authorization;

(6) Where applicable, a breakdown of what the surveillance technology was installed upon, including but not limited to on what vehicles or structures it was placed;

(7) Where applicable, a breakdown of what hardware surveillance technology software was installed upon;

(8) Where applicable, a breakdown of what databases the surveillance technology was applied to, including the frequency thereof;

(9) A summary of complaints or concerns that were received about the surveillance technology;

(10) The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response;

(11) An analysis of any discriminatory, disparate, and other adverse impacts the use of the technology may have had on the public's individual rights and liberties, including but not limited to those guaranteed by the First and Fourth, Amendment to the United States Constitution and [relevant sections of the state constitution's bill or rights]

(12) Statistics and information about public records act requests, including response rates; and

(13) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.

(B) Based upon information provided in the Annual Surveillance Report, the City Council shall determine whether the benefits of the surveillance technology outweigh its costs and whether the public's individual liberties and rights have been adequately protected and safeguarded. If the benefits do not outweigh the costs or individual rights and liberties have not been adequately protected and safeguarded, the City Council shall direct the use of the surveillance technology cease or shall require modifications to the Surveillance Use Policy that will resolve the observed failures.

Section 7

Not later than April 15 of each year, the City Council or its appointed designee shall release a public report, in paper and electronic form, containing the following information for the proceeding calendar year:

(A) The number of requests for approval submitted to the City Council under this Act for the funding, acquisition, or new use of surveillance technology;

(B) The number of times the City Council approved requests submitted under this Act for the funding, acquisition, or new use of surveillance technology;

(C) The number of times the City Council rejected requests submitted under this Act for the funding, acquisition, or new use of surveillance technology;

(D) The number of times the City Council requested modifications be made to Surveillance Impact Reports and Surveillance Use Policies before approving the funding, acquisition, or new use of surveillance technology; and

(E) All Annual Surveillance Reports submitted pursuant to Section 6.

Section 8

(A) Any violation of this Act, including but not limited to funding, acquiring, or utilizing surveillance technology that has not been approved pursuant to this Act or utilizing surveillance technology in a manner or for a purpose that has not been approved pursuant to this Act, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, writ of mandate, or evidence suppression in any court of competent jurisdiction to enforce this Act.

(B) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought to enforce this Act.

(C) Municipal employees or agents, except in response to a declared municipal, state, or federal state of emergency, shall not use any surveillance technology except in a manner consistent with policies approved pursuant to the terms of this Act, and may in no circumstances utilize surveillance technology in a manner which violates the City Charter, State Constitution, or United States Constitution. Any municipal employee who violates the provisions of this Act, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For municipal employees who are represented under the terms of a collective bargaining agreement, this Act prevails except where it conflicts with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

(D) Whistleblower protections.

> (1) No municipal entity or anyone acting on behalf of a municipal entity may take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment, including but not limited to discriminating with respect to compensation, terms, conditions, access to information, restrictions on due process rights, privileges of employment, or civil or criminal liability, because:
>
> > (a) The employee or applicant was perceived to, about to, or assisted in any lawful disclosure of information concerning the funding, acquisition, or use of a

surveillance technology or surveillance data to any relevant municipal agency, municipal law enforcement, prosecutorial, or investigatory office, or City Council Member, based upon a good faith belief that the disclosure evidenced a violation of this Act; or

(b) The employee or applicant was perceived to, about to, or assisted or participated in any proceeding or action to carry out the purposes of this Act.

(2) It shall be grounds for disciplinary action for a municipal employee or anyone else acting on behalf of a municipal entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this Act.

(3) Any employee or applicant who is injured by a violation of Section 8(D)(1) may institute a proceeding for monetary damages and injunctive relief in any court of competent jurisdiction.

(E) In addition, any person who:

(1) Knowingly violates this Act shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding $2,500 per violation, imprisonment of not more than six months, or both.

(2) Recklessly violates this Act shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding $1,000 per violation.

Section 9

It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that conflicts with the provisions of this Act, and any conflicting provisions in such contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. Conflicting provisions in contracts or agreements signed prior to the enactment of this Act shall be deemed void and legally unenforceable to the extent permitted by law. This section shall not apply to collective bargaining agreements and related memorandums of agreement or understanding that pre-date this Act.

Section 10

It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that facilitates the receipt of surveillance data from, or provision of surveillance data to any non-governmental entity in exchange for any monetary or any other form of consideration from any source, including the assessment of any additional fees, interest, or surcharges on unpaid fines or debts. Any contracts or agreements signed prior to the enactment of this Act that violate this section shall be terminated as soon as is legally permissible.

Section 11

The provisions in this Act are severable. If any part of provision of this Act, or the application of this Act to any person or circumstance, is held invalid, the remainder of this Act, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 12

This Act shall take effect on [DATE].