April 2021

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, the City Council finds that, while surveillance technology may threaten the privacy of all of us, throughout history, surveillance efforts have been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective.

WHEREAS, the City Council finds that decisions regarding if and how surveillance technologies should be funded, acquired, or used, and whether data from such technologies should be shared, should not be made until meaningful public input has been solicited and given significant weight.

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

WHEREAS, 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 civil rights and civil liberties safeguards have been strictly adhered to.

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

Section 1. City Council Approval Mandatory for Surveillance Technology Funding, Acquisition, or Use

(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 online, 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;

Comment [A1]: For any questions regarding this model bill, contact Chad Marlow at cmarlow@ACLU.org.

Comment [A2]: NOTE TO LOCALITIES: Throughout the document, make sure the proper name for your local legislative body is used. For Counties, "City" will also need to be replaced with "County" throughout.

Comment [A3]: NOTE TO LOCALITIES: Considerer adding references to relevant provisions of the State Constitution and/or City Charter here.

(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, including the sharing of surveillance data therefrom; 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.

Section 2. Surveillance Impact Report and Surveillance Use Policy Submission

(A) As a part of the process of seeking City Council approval, pursuant to Section 1(A), to fund, acquire, or use surveillance technology or to enter into an agreement concerning such funding, acquisition, or use, a municipal entity shall submit to the City Council and make publicly available a Surveillance Impact Report and Surveillance Use Policy concerning the technology at issue.

(1) No use of surveillance technology by a municipal entity pursuant to Section 1(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(A).

(2) Prior to approving or rejecting a Surveillance Impact Report or Surveillance Use Policy submitted pursuant to Section 2(A), the City Council may request revisions be made by the submitting municipal entity.

(B) Surveillance Impact Report: A Surveillance Impact Report submitted pursuant to Section 2(A) 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;

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

(3) If the surveillance technology will not be uniformly deployed or targeted throughout the city, what factors will be used to determine where the technology is deployed or targeted;

(4) The fiscal impact of the surveillance technology; and

(5) An assessment identifying with specificity:

(a) Any potential adverse impacts the surveillance technology, if deployed, might have on civil liberties and civil rights; and

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

(C) Surveillance Use Policy: A Surveillance Use Policy submitted pursuant to Section 2(A) 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) the surveillance technology is intended to advance.

(2) Authorized Use(s): For what specific capabilities and uses of the surveillance technology is authorization being sought, and

(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 but 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 entities or third parties seeking or demanding access to surveillance data.

(8) Auditing and Oversight: What mechanisms will be implemented to ensure the Surveillance Use Policy is followed, including 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.

(9) 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 how the municipal entity will ensure each question and complaint is responded to in a timely manner.

(D) The public City Council hearing required pursuant to Section 1(A) may not be held until the required Surveillance Impact Report and Surveillance Use Policy have been available to the public, at a designated page on the City website, for a period of at least twenty-one (21) calendar days.

Section 3. Review of Preexisting Uses Mandatory

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 that was in use prior to the effective date of this Act, or the sharing of surveillance data therefrom, must commence a City Council approval process in accordance with Section 1(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 submitted pursuant to Section 2(A), within one hundred eighty (180) days of its submission to the City Council, the municipal entity shall cease its use of the surveillance technology and the sharing of surveillance data therefrom until such time as City Council approval is obtained in accordance with this Act.

Section 4. Lead Entity Identification

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.

Section 5. Standard for Approval

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, that the proposal will safeguard civil liberties and civil rights, and that the uses and deployments of the surveillance technology will not be based upon discriminatory or viewpoint-based factors or have a disparate impact 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 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 civil rights or civil liberties has been identified in the Surveillance Impact Report pursuant to 2(B)(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. Annual Surveillance Report

(A) A municipal entity that obtains approval for the use of a surveillance technology must submit to the City Council, and make available on its public website, 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 and received from 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;

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

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

(6) An analysis of any discriminatory, disparate, and other adverse impacts the use of the technology may have had on the public's civil rights and civil liberties, including but not limited to those guaranteed by the First, Fourth, and Fourteenth Amendment to the United States Constitution; and

(7) 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) 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

Comment [A4]: NOTE TO LOCALITIES: Considerer adding references to relevant provisions of the State Constitution and/or City Charter here.

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 5. If it has not, the City Council shall direct the use of the surveillance technology be discontinued or shall require modifications to the Surveillance Use Policy that will resolve the observed failures.

(D) For purposes of this section, "external persons and entities" shall not include specifically identifying persons acting in their individual capacities.

Section 7. Annual Public Reporting

Not later than April 15 of each year, the City Council or its appointed designee shall release an annual public report, in print and on its public website, 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. Printed copies of the public report may contain pinpoint references to online locations where the Annual Surveillance Reports are located, in lieu of reprinting the full reports.

Section 8. Community Advisory Committee on Surveillance

(A) Within three (3) months of the adoption of this Act, the City Council shall appoint a Community Advisory Committee on Surveillance to provide the City Council with broad principles to help guide decisions about if and how surveillance technologies should be used by the City and its municipal agencies.

(1) The membership of the Community Advisory Committee on Surveillance should reflect the diversity of the City's residents, and special efforts should be made to ensure communities that have historically been disproportionately subjected to government surveillance are well-represented.

(2) The Community Advisory Committee on Surveillance shall have a Chair and Vice Chair, who shall be elected annually by the members of the Committee.

(B) Every year, by no later than September 15, the Community Advisory Committee on Surveillance shall produce and submit to the City Council a Surveillance Technology Community Equity Impact Assessment and Policy Guidance, which shall address, at a minimum, the following:

(1) What communities and groups in the City, if any, are disproportionately impacted by the use of surveillance technologies, what disparities were perceived and/or experienced, and what were the resulting adverse impacts on the community's or group's civil rights and/or civil liberties;

(2) With respect to each perceived or experienced disparity identified in response to Section 8(B)(1), what remedial adjustments to laws and policies, including but not limited to prior approvals granted pursuant to Section 1(A), should be made so as to achieve a more just and equitable outcome in the future.

(3) With respect to each remedial adjustment identified in response to Section 8(B)(2), what additional funding, implementation strategies, and/or accountability mechanisms would be needed to effectuate the adjustment; and

(4) In light of the collective responses to Section 8(B)(1)-(3), what new approaches and considerations should the City Council bring to future reviews of applications submitted pursuant to Section 1(A).

Section 9. Remedies; Penalties; Whistleblower Protections; Exclusionary Rule; Deletion/Destruction Requirement

(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 is discriminatory, viewpoint-based, or violates the City Charter, State Constitution, or United States Constitution.

Comment [A5]: NOTE TO LOCALITIES: Insert proper name if "City Charter" is not the name used by your city.

(D) Any person who knowingly violates this Act shall be deemed guilty of a misdemeanor and may be punished by a fine not exceeding $2,500 per violation.

(1) For purposes of this subsection, a "violation" shall constitute each and every individual acquisition, deployment, and use of a surveillance technology or the data therefrom in violation of this Act.

(E) 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 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.

(F) Exclusionary Rule; Deletion/Destruction Requirement

(1) Any data or other information created or collected in contravention of this Act, and any data or information derived therefrom, shall be immediately deleted and destroyed, and may not:

(a) Be offered as evidence by any City government entity, agency, department, prosecutorial office, or any other subdivision thereof, in any criminal or civil action or proceeding against any member of the public, except as evidence of the violation of this Act; or

(b) Be voluntarily provided to another person or entity for use as evidence or for any other purpose.

(2) Notwithstanding the above, if, upon the discovery of data or other information that was created or collected in contravention of this Act, it appears such data or information may be material to the defense in a criminal prosecution, a copy of the relevant, potentially material data or other information shall be turned over to the defendant before it is deleted and destroyed.

Section 10. Conflicting Contractual Agreements Prohibited

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.

Section 11. Certain Public-Private Contracts Prohibited

It shall be unlawful for the city or any municipal entity to enter into any contract or other agreement that facilitates the receipt of privately generated and owned surveillance data from, or provision of government generated and owned 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 12. Definitions

For the purposes of this Act:

(A) "Discriminatory" shall mean (1) disparate treatment of any individual(s) because of any real or perceived traits, characteristics, or status as to which discrimination is prohibited under the Constitution or any law of the United States, the constitution or any law of the State of XXX, or the City Charter or any law of the City of YYY, or because of their association with such individual(s), or (2) disparate impact on any such individual(s) having traits, characteristics, or status as described in subsection (1).

(B) "Disparate impact" shall mean an adverse effect that is disproportionately experienced by individual(s) having any traits, characteristics, or status as to which discrimination is prohibited under the Constitution or any law of the United States, the constitution or any law of the State of XXX, or the City Charter or any law of the City of YYY than by similarly situated individual(s) not having such traits, characteristics, or status.

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

(D) "New surveillance technology" shall mean any type of surveillance technology, the acquisition of which was not previously approved by the City Council. A surveillance technology is not considered a new surveillance technology where its capabilities and functionality do not differ in any significant way from a previously approved version of an equivalent surveillance technology.

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

(F) "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, behavioral, 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 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

Comment [A6]: NOTE TO LOCALITIES: Insert state name here.

Comment [A7]: NOTE TO LOCALITIES: Insert proper name if "City Charter" is not the name used by your city.

Comment [A8]: NOTE TO LOCALITIES: Insert city name here.

Comment [A9]: NOTE TO LOCALITIES: Insert state name here.

Comment [A10]: NOTE TO LOCALITIES: Insert proper name if "City Charter" is not the name used by your city.

Comment [A11]: NOTE TO LOCALITIES: Insert city name here.

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 12(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 surveillance-related functions; (b) Parking Ticket Devices (PTDs); (c) 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.

(G) "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 or 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 14. Effective Date

This Act shall take effect on [DATE].