BOARD BILL NO. 66 SPONSORED BY: ALDERMAN TERRY KENNEDY, ALDERMAN JOHN COLLINS MUHAMMAD

An Ordinance setting out regulations regarding the use of surveillance technology by the City of St. Louis, requiring the submission of Surveillance Program Plans and review by the Board of Aldermen before such plans can be put into practice; and containing a severability clause and an emergency clause.

WHEREAS, surveillance technology is becoming an increasingly common, supportive, and helpful mechanism in maintaining public safety, peace, and welfare; and

WHEREAS, these technologies include various types and sizes of cameras, internet surveillance programming, listening devices, phone monitoring systems and other technologies; and

WHEREAS, a number of academic studies, legal opinions, and scholarly reports have all cited the balance that must be struck between the use of surveillance technologies and the civil rights and liberties of U.S. citizens living in a free democratic society; and

WHEREAS, a number of studies have shown that surveillance technologies are developing faster than the laws to govern them, resulting in an imbalance between governance and the use of these technologies and causing several cities across the country to enact new and/or revised statutes to ensure the civil rights and liberties of its citizens while allowing lawful surveillance as a viable safety option.

BE IT ORDAINED BY THE CITY OF ST. LOUIS AS FOLLOWS:

SECTION ONE. Definitions:

(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 Missouri, or the Charter or any ordinance of the City of St. Louis, 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 this section.

(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, under the Constitution or any law of the State of Missouri, or under the Charter or any ordinance of the City of St. Louis.

(C) "City entity" shall mean any St. Louis City government, agency, department, bureau, division, board, commission, committee, or unit of the City of St. Louis.

(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 device, hardware, or

software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing captured-while-live 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 or used as such a 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 light bulbs 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

City 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 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 unless such recorders are used as surveillance technology surreptitiously and/or without a warrant; (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.

(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.

(G) "Surveillance Program" any shall mean physical or digital system, routine,

or process designed for the close watch and/or continual observation or tracking of a person or group suspected of doing something illegal or for general public safety and welfare. If a given tactic, such as stakeouts or physical tracking, is used repeatedly, the tactic as a whole shall be considered a Surveillance Program rather than individual instances of the tactic.

SECTION TWO. Surveillance Program Usage.

All Surveillance Programs conducted by any City entity shall be for the public safety and welfare as well as to protect public and individual civil rights and liberties.

SECTION THREE. Surveillance Program Plans.

Any City entity that determines to have, operate, contract, borrow, share, participate in and/or create a Surveillance Program, modify the use, functionality or capacity of an existing Surveillance Program, or enter into an agreement involving mutual assistance in which personnel using such technology are shared inter-jurisdictionally, shall first create a Surveillance Program Plan that shall be submitted to the Board of Aldermen for approval before implementation. The Surveillance Program Plan shall include the following:

1. The reason and need for the program.

2. The identified target area, and/or group, such as wards or neighborhoods, the factors and methods used in determining targets, and how this relates to the need and the reason for the program.

3. Desired and planned outcomes.

4. The City entity, contracted parties or other cooperating agencies or entities involved.

5. The lead City entity making the plan and administering the program.

6. If any aspects of the program will be delegated to any other City entity other than the lead City entity.

7. The surveillance techniques to be used including the specific type of equipment including product descriptions from the manufacturer, the duration of the program, and time periods of surveillance such as daylight hours, nighttime hours or extended days.

8. A surveillance usage policy that includes usage of data, who shall handle and have access to the information, storage of information and how civil rights and liberties are to be protected. The usage policy shall include, but not be limited to:

a) What rules will govern, and what processes will be required prior to each action of the Surveillance Program, including but not limited to:

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

ii) Whether a judicial warrant is required; and

iii) What information must be included in any warrant or court authorization granting permission to use the device to ensure, among other things, that the court is well and fully informed about the technology or technique, their functionality, and the uses for which judicial authorization is being sought;

b) What potential capabilities and uses of the surveillance technology or techniques will be prohibited, such as the warrantless surveillance of non-public

spaces;

c) The extent to which, and how, the Surveillance Program will be used to monitor persons in real time, as data is being captured;

d) Whether the Surveillance Program will be used to investigate (i) violent crimes, (ii) non-violent crimes, (iii) felonies, (iv) misdemeanors, and (v) other legal or code violations, infractions not classified as felonies or misdemeanors, unlawful activity, activities or patterns considered to be indicators of potential future involvement in criminal activity, or perceived or actual gang or other group affiliations;

e) The extent to which, how, and under what circumstances retained surveillance data that was collected, captured, recorded, or intercepted by the Surveillance Program will be analyzed or reviewed;

f) Under what limited circumstances an individual will be allowed to access 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 the acceptable grounds are for gaining access to the surveillance data;

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

h) What procedures will be put in place to prevent the unauthorized distribution of the copied surveillance data;

i) What safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms; and

j) What rules and procedures will govern the retention of surveillance data, including:

i) For what standard, 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 Program Plan;

ii) What specific conditions must be met to retain surveillance data beyond the standard retention period;

iii) By what process surveillance data will be regularly deleted after the standard retention period elapses and what auditing procedures will be implemented to ensure data is not improperly retained beyond the standard retention period;

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

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

vi) 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 improperly collected or retained surveillance data, including any copies thereof, will be expeditiously destroyed once it is identified;

vii) 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

viii) 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."

9. Initial and ongoing costs of the program and the income sources to be used, including any in kind donations.

10. Impact Study and Review that includes:

a) how civil rights and liberties could potentially be affected, which groups might be so affected, which groups or geographical areas might receive disproportionate activity, and how civil rights and liberties are to be protected in those instances;

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, including expeditious identification and deletion;

c) potential harms that could be caused by intentional or inadvertent

actions conducted in a discriminatory or viewpoint-based manner;

d) impacts caused by faulty or biased algorithms;

e) potential impacts on privacy; and

f) where applicable, what databases the technology will rely upon to make subject identifications, whether any biases exist within any of the identified databases, and how, if any biases exist within an identified database, the database can be used without incorporating those biases.

11. How and when surveillance data will be accessible to members of the public, how the City entity interprets the applicability of, and intends to comply with Chapter 610 of the Revised Statutes of Missouri with respect to surveillance data, and what steps will be taken to protect individual privacy.

12. How, to what extent, and when surveillance data, in accordance with applicable law, will be accessible to targets of criminal or civil investigations, criminal or civil plaintiffs or defendants, and their attorneys.

13. If a City entity intends to share access to surveillance technology or surveillance data with any other governmental personnel, agencies, departments, bureaus, divisions, or units.

14. How such sharing is necessary for the stated purpose and use of the surveillance technology.

15. How the Surveillance Program Plan will ensure any entity sharing access to the surveillance technology or surveillance data complies with the applicable Surveillance Program Plan and does not further disclose the surveillance data to unauthorized persons and entities.

16. What legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.

17. What processes will be used to guarantee that the City entity seeks approval for future surveillance technology or surveillance data sharing agreements from the Board of Aldermen.

18. What processes will be used to guarantee that the City entity seeks approval from the Board of Aldermen before granting permission through an inter-jurisdictional agreement to employees or agents of a municipal agency from another local-level jurisdiction, including but not limited to a municipality or county, to use any surveillance technology inside the geographical boundaries of the City of St. Louis, or to target any geographical locations or persons located inside the geographical boundaries of the City of St. Louis, and that such technology is previously approved for the City of St. Louis in accordance with this ordinance.

19. What unit or individuals will be responsible for ensuring compliance with the Surveillance Program Plan, and when and how compliance audits will be conducted.

20. What mechanisms will be implemented to ensure the Surveillance Program Plan is followed, including what internal personnel will be assigned to ensure compliance with the policy.

21. What independent persons or entities will be given oversight authority, and what legally enforceable sanctions will be put in place for individuals who violate the policy.

22. What training, including training materials, will be required for any individual authorized to use the surveillance technology or to access surveillance data, so as to ensure compliance with all applicable laws and regulations.

23. 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; what internal personnel will be assigned to receive, register, track, and respond to such communications; and how the City entity will ensure each question and complaint is properly responded to and addressed in a timely manner.

SECTION FOUR. Program Approval.

1. Approval:

A City entity must obtain Board of Aldermen approval by resolution before entering into a contract for or implementing any Surveillance Program Plan.

2. Public Input:

a) Within sixty (60) days, but not less than thirty (30) days, of submitting a Surveillance Program Plan, the City entity 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 Surveillance Program Plan. Such meetings shall not be held within a law enforcement facility.

b) Not less than 30 days after the City entity's public hearing and any revisions made to the Surveillance Program Plan, the Board of Aldermen

shall hold one or more public hearings at which the public is afforded a fair and adequate opportunity to provide online, written, and oral testimony prior to taking any action upon the Surveillance Program Plan. The head or representative of the City entity making the plan shall also be in attendance at this meeting to review the plan and answer questions. If changes are made to the plan after the first hearing, a subsequent public hearing shall be held by the Board of Aldermen allowing for public comment and after a notice published seven days prior. The Board of Aldermen may not take action until these hearings are held.

3. Public Hearing Notice: The Board of Aldermen shall give a 30-day notice of the first hearing on any Surveillance Program Plan and a 14-day notice for subsequent hearings.

4. Copies of Surveillance Program Plan: The City entity submitting a Surveillance Program Plan shall make an electronic copy of the plan available to the Board of Aldermen when they make submission to them and the number of copies requested by the Chair of the Committee designated by the Board of Aldermen to hold the hearing.

5. Program Plan Made Available: The Board of Aldermen shall make copies of the Program Plan available for review by the public at least 15 days before the public hearing. Changes made to any program plan after the first hearing shall be made available for public review 14 days before the Board of Aldermen holds the required public hearing allowing for public comment.

6. Notwithstanding the provisions of Section Four and pursuant to Sections 610.021 and 610.022 of the Missouri Revised Statutes, all information required in this ordinance which an agency may close under these Sections shall be designated as open.

SECTION FIVE. Compliance.

No later than one hundred twenty (120) days following the effective date of this ordinance any City entity seeking to continue the use of any presently used surveillance technology or techniques that were in use prior to the effective date of this ordinance must submit a Surveillance Program Plan to the Board of Aldermen. This includes any existing agreements to borrow or share surveillance technology, including mutual assistance in which personnel using such technology are shared inter-jurisdictionally. The Board of Aldermen shall make a determination to approve or disapprove within 180 days after the City entity has submitted a Surveillance Program Plan to the Board. Such City entity must receive Board of Aldermen approval in accordance with the processes of this ordinance to continue its Surveillance Program.

SECTION SIX. Approvals.

The Board of Aldermen shall only approve a request to fund, acquire, or use a surveillance technology and/or establish a Surveillance Program if it determines the benefits of the surveillance technology outweigh its costs (including non-financial costs), that the plan 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. An approval for the Surveillance Program Plan by the Board of

Aldermen, where the risk of potential adverse impacts on civil rights or civil liberties has been identified in the Surveillance Program Plan, 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 SEVEN. Annual Report.

1. A City entity that obtains approval for the use of surveillance technology must submit to the Board of Aldermen, and make available on its public website and in printed form free of charge, an Annual Surveillance Report for each specific Surveillance Program used by the City entity annually on or before March 15. The Annual Surveillance Report shall, at a minimum, include the following information for the previous calendar year:

a) A summary of how the surveillance technology and techniques were used;

b) 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);

c) Where applicable, a breakdown of where the surveillance technology and techniques were deployed geographically, by ward. For each ward, the City entity shall report how many individual days the surveillance technology and techniques were deployed and what percentage of those daily-reported deployments were subject to (A) a warrant, and (B) a non-warrant form of court authorization;

d) Where applicable, a breakdown of how many times the surveillance technology and techniques were used to investigate potential or actual (A) violent crimes, (B) non-violent crimes, (C) felonies, (D) misdemeanors, and (E) other legal or code violations, infractions not classified as felonies or misdemeanors, unlawful activity, activities or patterns considered to be indicators of potential future involvement in criminal activity;

e) Where applicable, and with the greatest precision that is reasonably practicable, the amount of time the surveillance technology and techniques were 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;

f) 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;

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

h) Where applicable, a breakdown of what databases the surveillance technology and techniques were applied to, including the frequency thereof;

i) A summary of complaints or concerns that were received about the surveillance technology and techniques;

j) The results of any internal audits, any information about violations of the Surveillance Program Plan, and any actions taken in response;

k) An analysis of any discriminatory, disparate, and other adverse impacts the use of the technology and techniques 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 Amendments to the United States Constitution, the Missouri Constitution, and St. Louis City Charter;

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

m) Total annual costs for the surveillance technology and techniques, including personnel and other ongoing costs, and what source will fund the technology in the coming year;

n) If there was a State of Emergency or other State or Federal override and what impacts it had, how long it lasted, what ongoing use was/is being made of the data;

o) The number of Surveillance Program Plans submitted during the previous year;

p) Number of breakdowns, repairs and replacement of equipment; and

q) Any recommended changes for the future use of the Surveillance Program and the relevant changes the City entity considers necessary to make to the Surveillance Program Plan.

2. Based upon information provided in the Annual Surveillance Report and public hearings that follow the same process outlined for approval of the Surveillance Program Plan, the Board of Aldermen shall determine whether the benefits of the Surveillance Program outweigh its costs and whether the public's civil liberties and civil

rights have been adequately protected and safeguarded. In making this determination, the Board of Aldermen may request testimony from any entity that oversees any aspect of the Surveillance Program. If the benefits do not outweigh the costs, or civil rights and civil liberties have not been adequately protected and safeguarded, or the Board of Aldermen determines that the Surveillance Program could be improved, the Board of Aldermen may direct that the use of the Surveillance Program cease or shall require modifications to Surveillance Program Plan that will resolve the observed failures.

SECTION EIGHT. Changes.

If, during the course of the year and before an Annual Surveillance Report has been submitted, the City entity administering a Surveillance Program requests changes to its program or the Board of Aldermen determines that changes need to be made to the Surveillance Program Plan, the Board of Aldermen may make such changes and/or approvals, pursuant to the public notice and hearing requirements outlined in this ordinance.

SECTION NINE. Unlawful Use.

1. Conflicts in Contracts and Agreements. It shall be unlawful for the City of St. Louis or any City 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.

2. Non-Governmental Entities. It shall be unlawful for the City of St. Louis or

any City 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.

3. Surveillance data that has been improperly collected and/or retained shall not be used in court.

SECTION TEN. Severability.

The provisions in this ordinance 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.