ORDINANCE NO XX
DATE OF FINAL PASSAGE ____

TRANSPARENT AND RESPONSIBLE USE OF SURVEILLANCE TECHNOLOGY ORDINANCE

AN ORDINANCE ESTABLISHING RULES FOR THE CITY'S ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGY

WHEREAS, the City of San Diego has recognized the importance of open data for an informed public debate and the creation of improved knowledge, technologies, and services;

WHEREAS, the City Council finds that the installation of surveillance technology may hinder the privacy of San Diego residents; and the City's acquisition, installation and use of surveillance technology is a question of public consequence for democracy and governance;

WHEREAS, emergent technologies can promise valuable approaches but can also balloon in unexpected costs, thus responsible adoption requires prudent analysis of fiscal and social costs and benefits;

WHEREAS, San Diego City Council acknowledges the privacy rights of its individual citizens, it also recognizes that surveillance technology may be a valuable tool to support community safety and investigation and prosecution of crimes; and

WHEREAS, San Diego Police Department is accountable to this municipality; responsible for its public safety while granted limited resources; and charged with a mission to serve and protect its residents, rather than to monitor, harass, or intimidate them;

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and awareness that the Government may be watching chills associational and expressive freedoms; and awareness that social control can operate through behavioral data targeting rather than privacy violations.

WHEREAS, we recognize the historical use of surveillance data — both by design or in ways unintended by policy — to intimidate and oppress certain 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 no decisions relating to the City's use of 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 California and United States Constitutions; and

WHEREAS, the City Council finds that any and all decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public concern should be given significant weight in policy decisions; and

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 City 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 the public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

NOW, THEREFORE, BE IT ORDAINED by the Council that the City of San Diego adopts the following:

Transparent and Responsible Use of Surveillance Technology Ordinance which hereby establishes processes for creating transparency, accountability, and public deliberation informing the City's acquisition and usage of surveillance technology.

SECTION 1. Definitions

The following definitions apply to this Section:

1. "Commission" means the Privacy Advisory Commission established by the Privacy Advisory Commission Ordinance (###) (hereinafter referred to as the "Privacy Commission" or "Commission").
2. "Annual Surveillance Report" means a written report concerning a specific surveillance technology that includes all the following:
    A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology;
    B. Whether and how often data acquired through the use of the surveillance technology was shared with any entities (e.g. internal or external), the name of any

recipient 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 what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to;
D. A list of any software updates, hardware upgrades, or system configuration changes accompanied by a description of altered or improved functionality that resulted in the expansion or contraction of system access, data retention, or data access, as well as a description of the reason for the change.
E. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each Police Area in the relevant year;
F. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall identify the race of each person that was subject to the technology's use.
G. The results of any internal audits or investigations, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response (unless the release of such information is prohibited by law, including but not limited to confidential personnel file information, in which case the omission and its cause should be reported).
H. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;
I. Description of all methodologies used to detect incidents of data breaches or unauthorized access;
J. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes;
K. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates;
L. 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; and
M. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

3. "City" means any department, agency, bureau, and/or subordinate division of the City of San Diego as stated in the Charter.

4. “City staff” means City personnel authorized by the City Administrator or designee to seek City Council Approval of Surveillance Technology in conformance with this Chapter.

5. “Continuing agreement” means an agreement that automatically renews unless terminated by one party.

6. “Facial recognition technology” means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face.

7. “Personal communication device” means a mobile telephone, a personal digital assistant, a wireless capable tablet and a similar wireless two-way communications and/or portable Internet accessing devices, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of City business.

8. “Police Area” refers to each of the geographic districts assigned to a police commander and as such districts are amended from time to time.

9. “Surveillance” or “surveil” means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be revealed by data or combinations of data, such as license plate data, images, IP addresses, user ids, unique digital identifier, or data traces left by the individual.

10. “Surveillance technology” means any software (e.g. scripts, code, Application Programming Interfaces), electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to observe, collect, retain, analyze, process, or share audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. It also includes the product (e.g., audiovisual recording, data, analysis, report) of such surveillance technology. Examples of surveillance technology include, but is not limited to the following: cell site simulators (Stingrays); automatic license plate readers; gunshot detectors (ShotSpotter); drone-mounted data collection; facial recognition technology; thermal imaging systems; body-worn cameras; social media analytics software; gait analysis software; video cameras that record audio or video, and transmit or can be remotely accessed. It also includes software designed to monitor social media services or forecast criminal activity or criminality, biometric identification hardware or software.

A. “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 above:

1. Routine office hardware, such as televisions, computers, credit card machines, badge readers, copy machines, and printers, that is in widespread use and will not be used

for any surveillance or law enforcement functions;

2. Parking Ticket Devices (PTDs);

3. 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;

4. Surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles;

5. Manually-operated technological devices used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems;

6. City databases that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases.

7. Medical equipment used to diagnose, treat, or prevent disease or injury, unless the equipment generates information that can be used to identify individuals.

8. Police department interview room cameras.

9. Police department case management systems.

10. Personal Communication Devices that have not been modified beyond stock manufacturer capabilities in a manner described above.

11. "Community Meeting" means a publicly held meeting that is accessible, noticed in multiple languages, for the purpose of educating communities, answering questions, and learning about potential impacts on disadvantaged groups.

12. "Surveillance Impact Report" means a publicly posted written report including at a minimum the following:

A. Description: Information describing the surveillance technology and how it works, including product descriptions from manufacturers;
B. Purpose: Information on the proposed purposes(s) and outcomes for the surveillance Technology;
C. Location: The physical or virtual location(s) it may be deployed, using general descriptive terms, and crime statistics for any location(s);
D. Impact: An assessment of the technology's adopted use policy and whether it is adequate in protecting civil rights and liberties and whether the surveillance technology was used or deployed, intentionally or inadvertently, in a manner that is discriminatory (disparate impacts on marginalized communities), viewpoint-based, or biased via algorithm;
E. Mitigations: Identify specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each such impacts;
F. Data Types and Sources: A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports,

logic or algorithm used, and any additional information derived therefrom;

G. Data Security: Information about the controls that will be designed and implemented to ensure that security objectives are achieved to safeguard the data collected or generated by the technology from unauthorized access or disclosure;
H. Fiscal Cost: The forecasted, prior, and ongoing fiscal costs for the surveillance technology, including initial purchase, personnel, and other ongoing costs, and any current or potential sources of funding;
I. Third Party Dependence: Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor at any time;
J. Alternatives: A summary of all alternative methods (whether involving the use of a new technology or not) considered before deciding to use the proposed surveillance technology, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate; and,
K. Track Record: A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses), existing publicly reported controversies, and any court rulings in favor or in opposition to the technology.
L. Public engagement and comments: A description of any community engagement held and any future community engagement plans, number of attendees, a compilation of all comments received and departmental responses given, and departmental conclusions about potential neighborhood and disparate impacts that may result from the acquisition.

13. "Surveillance Use Policy" means a publicly-released and legally enforceable policy for use of the surveillance technology that at a minimum specifies the following:

A. Purpose: The specific purpose(s) that the surveillance technology is intended to advance;
B. Authorized Use: The specific uses that are authorized, the rules and processes required prior to such use, as well as a description of controls used to prevent or detect circumvention of those rules and processes;
C. Data Collection: The information that can be collected, captured, recorded, intercepted or retained by the surveillance technology, as well data that might be inadvertently collected during the authorized uses of the surveillance technology and what measures will be taken to minimize and delete such data. Where applicable, list any data sources the technology will rely upon, including “open source” data;
D. Data Access: The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the

information as well as a description of controls used to prevent or detect circumvention of rules and processes;

E. Data Protection: The safeguards that protect information from unauthorized access, including system logging, encryption, and access control mechanisms;
F. Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period;
G. Public Access: How collected information can be accessed or used by members of the public, including criminal defendants;
H. Third Party Data Sharing: If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;
I. Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology;
J. Auditing and Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy; and
K. Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.
L. Complaints: The procedures that 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.

SECTION 2. Privacy Advisory Commission (PAC) Notification and Review Requirements

1. PAC Notification Required Prior to City Solicitation of Funds and Proposals for Surveillance Technology.
    A. City staff shall notify the Chair of the Privacy Advisory Commission prior to:
        1. Seeking or soliciting funds for surveillance technology or the information it provides, including but not limited to applying for a grant; or,
        2. Soliciting proposals with any entity to acquire, share or otherwise use

surveillance technology or the information it provides.

3. Otherwise, formally, or informally, facilitating or implementing surveillance technology in collaboration with other entities, including city entities;

B. Upon notification by City staff, the Chair of the Privacy Advisory Commission shall place the item on the agenda at the next Privacy Advisory Commission meeting for discussion and possible action. At this meeting, City staff shall inform the Privacy Advisory Commission of the need for the funds or equipment, or shall otherwise justify the action City staff will seek Council approval for pursuant to <§3.1.>. The Privacy Advisory Commission may make a recommendation to the City Council by voting its approval to proceed, object to the proposal, recommend that the City staff modify the proposal, or take no action.

C. Should the Privacy Advisory Commission not make a recommendation pursuant to <§2.1.B>, City staff may proceed and seek Council Approval of the proposed Surveillance Technology initiative pursuant to the requirements of <§3.1.>.

2. PAC Review Required for New Surveillance Technology Before City Council Approval

A. Prior to seeking City Council approval under <§3.1.>, City staff shall submit a Surveillance Impact Report and a Surveillance Use Policy for the proposed new surveillance technology initiative to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under <§1.10>.

Prior to submitting the Surveillance Impact Report, the department must complete one or more community meetings defined in <§1.11> in each council district with opportunity for public comment and written response. The Council may direct the department to conduct additional community engagement before approval, or after approval as a condition of approval.

B. The Privacy Advisory Commission shall recommend that the City Council adopt, modify, or reject the proposed Surveillance Use Policy. If the Privacy Advisory Commission proposes that the Surveillance Use Policy be modified, the Privacy Advisory Commission shall propose such modifications to City staff. City staff shall present such modifications to City Council when seeking City Council approval under <§3.1.>.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the item.

3. PAC Review Requirements for Existing Surveillance Technology Before City Council Approval

A. Prior to seeking City Council approval for existing City surveillance technology under <§3.1.> City staff shall submit a Surveillance Impact Report and Surveillance Use Policy for each existing surveillance technology to the Privacy Advisory Commission for its review at a regularly noticed meeting. The Surveillance Impact Report and Surveillance Use Policy must address the specific subject matter specified for such reports as defined under <§1.10.>.

Prior to submitting the Surveillance Impact Report, the department must complete one or more community meetings defined under <§1.11> in each council district with opportunity for public comment and written response. The Council may direct the department to conduct additional community engagement before approval, or after approval as a condition of approval.

B. Prior to submitting the Surveillance Impact Report and proposed Surveillance Use Policy as described above, City staff shall present to the Privacy Advisory Commission a list of surveillance technology possessed and/or used by the City.

C. The Privacy Advisory Commission shall rank the items in order of potential impact to civil liberties.

D. Within sixty (60) days of the Privacy Advisory Commission's action in < §2.3.C>, City staff shall submit at least one (1) Surveillance Impact Report and proposed Surveillance Use Policy per month to the Privacy Advisory Commission for review, beginning with the highest-ranking items as determined by the Privacy Advisory Commission, and continuing thereafter each month until a Surveillance Impact Report and Surveillance Use Policy has been submitted for each item on the list.

E. Failure by the Privacy Advisory Commission to make its recommendation on any item within 90 days of submission shall enable City staff to proceed to the City Council for approval of the item pursuant to <§3.1>.

SECTION 3. City Council Approval Requirements for New and Existing Surveillance Technology

1. City staff must obtain City Council approval prior to any of the following:

A. Accepting local, state, federal funds or in-kind or other donations for surveillance technology;

B. Acquiring new surveillance technology, including but not limited to procuring such technology without the exchange of monies or consideration;

C. Using new surveillance technology, or using existing surveillance technology or the information it provides for a purpose, in a manner or in a location not previously approved by the City Council pursuant to the requirements of this ordinance; or

D. Entering into a continuing agreement or written agreement to acquire, share or otherwise use surveillance technology or the information it provides, including data sharing agreements.

2. City Council Approval Process

A. After the PAC Notification and Review requirements in <§2> have been met, City staff seeking City Council approval shall schedule for City Council consideration and approval of the proposed Surveillance Impact Report and proposed Surveillance Use Policy, and include Privacy Advisory Commission recommendations at least fifteen (15) days prior to a mandatory, properly-noticed, germane public hearing. Approval may only occur at a public hearing.

B. The City Council shall only approve any action as provided in this Chapter after first considering the recommendation of the Privacy Advisory Commission, and subsequently making a determination that the benefits to the community of the surveillance technology outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the City Council's judgment, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective.

C. For Approval of Existing Surveillance Technology for which the Privacy Advisory Commission failed to make its recommendation within ninety (90) days of review as provided for under <§2.3.E>, if the City Council has not reviewed and approved such item within four City Council meetings from when the item was initially scheduled for City Council consideration, the City shall cease its use of the surveillance technology until such review and approval occurs.

3. Surveillance Impact Reports and Surveillance Use Policies are Public Records

City staff shall make all Surveillance Impact Reports and Surveillance Use Policies, as updated from time to time, available to the public as long as the City uses the surveillance technology.

All Surveillance Impact Reports and Surveillance Use Policies must be posted to the City's website

with an indication of its current approval status and the planned City Council date for action.

SECTION 4. Oversight Following City Council Approval

1. For each approved surveillance technology item, City staff must present an Annual Surveillance Report for Privacy Advisory Commission review a year from the date of City Council approval of said technology and annually thereafter as long as the technology is in use.

If City staff is unable to meet the annual deadline, City staff shall notify the Privacy Advisory Commission in writing of staff's request to extend this period, and the reasons for that request. The Privacy Advisory Commission may grant a single extension of up to sixty (60) days to comply with this provision.

A. After review of the report by the Privacy Advisory Commission, City staff shall submit the Annual Surveillance Report to the City Council.

B. The Privacy Advisory Commission shall recommend to the City Council that the benefits to the community of the surveillance technology in question outweigh the costs and that civil liberties and civil rights are safeguarded; that use of the surveillance technology cease; or propose modifications to the corresponding Surveillance Use Policy that will resolve the concerns.

C. Failure by the Privacy Advisory Commission to make its recommendation on the item within 90 days of submission shall enable the City entity to proceed to the City Council for approval of the Annual Surveillance Report.

D. In addition to the above submission of any Annual Surveillance Report, City staff shall provide in its report to the City Council a summary of all requests for City Council approval pursuant to <§3.1> and the pertinent Privacy Advisory Commission recommendation, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval.

2. Based upon information provided in City staff's Annual Surveillance Report and after considering the recommendation of the Privacy Advisory Commission, the City Council shall re-visit its "cost benefit" analysis as provided in <§3.2.B> and either uphold or set aside the previous determination. Should the City Council set aside its previous determination, the City's use of the surveillance technology must cease. Alternatively, City Council may require modifications to the Surveillance Use Policy that will resolve any deficiencies.

SECTION 5. Enforcement

1. Violations of this article are subject to the following remedies:

A. Any violation of this Ordinance, or of a Surveillance Use Policy promulgated under this Ordinance, constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Ordinance. An action instituted under this paragraph shall be brought against the respective City department, and the City of San Diego, and, if necessary to effectuate compliance with this Ordinance or a Surveillance Use Policy (including to expunge information unlawfully collected, retained, or shared thereunder), any other governmental agency with possession, custody, or control of data subject to this Ordinance, to the extent permitted by law.

B. Any person who has been subjected to a surveillance technology in violation of this Ordinance, or of a Surveillance Use Policy, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Ordinance or of a Surveillance Use Policy promulgated under this Ordinance, may institute proceedings in the Superior Court of the State of California against the City of San Diego and shall be entitled to recover actual damages (but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater).

C. A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in; an action brought under paragraphs (A) or (B).

D. Violations of this Ordinance by a City employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any Memorandums of Understanding with employee bargaining units.

SECTION 6. Secrecy of Surveillance Technology

It shall be unlawful for the City to enter into any surveillance-related contract or other agreement that conflicts with the provisions of this Ordinance, and any conflicting provisions in such existing or future contracts or agreements, including but not limited to non-disclosure agreements, shall be deemed void and legally unenforceable. To the extent permitted by law, the City shall publicly disclose all of its surveillance-related contracts, including any and all related non-disclosure agreements, if any, regardless of any contract terms to the contrary.

SECTION 7. Whistleblower Protections

1. Neither the City nor anyone acting on behalf of the City 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 and conditions of employment, access to information, restrictions on due process rights, 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 surveillance technology or surveillance data based upon a good faith belief that the disclosure evidenced a violation of this Ordinance; 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 Ordinance.

2. It shall be grounds for disciplinary action for a City employee or anyone else acting on behalf of the City to retaliate against another City employee or applicant who makes a good-faith complaint that there has been a failure to comply with any Surveillance Use Policy or Administrative Instruction promulgated under this Ordinance.

3. Any employee or applicant who is injured by a violation of this section may institute a proceeding for monetary damages and injunctive relief against the City in any court of competent jurisdiction.

SECTION 8. Severability

If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause, or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses, or phrases may be declared invalid or unconstitutional.

SECTION 9. Effective Date

This ordinance shall become effective immediately on final adoption if it receives five or more affirmative votes; otherwise it shall become effective upon the seventh day after final adoption.

ORDINANCE NO XX
DATE OF FINAL PASSAGE ____

PRIVACY ADVISORY COMMISSION ORDINANCE

AN ORDINANCE ESTABLISHING A PRIVACY ADVISORY COMMISSION, PROVIDING FOR THE APPOINTMENT OF MEMBERS THEREOF, DEFINING THE DUTIES AND FUNCTIONS OF SAID COMMISSION

WHEREAS, the City of San Diego has recognized the importance of open data for an informed public debate and the creation of improved knowledge, technologies, and services;

WHEREAS, the City Council finds that the installation of surveillance technology may hinder the privacy of San Diego residents; and the City's acquisition, installation and use of surveillance technology is a question of public consequence for democracy and governance;

WHEREAS, emergent technologies can promise valuable approaches but can also balloon in unexpected costs, thus responsible adoption requires prudent analysis of fiscal and social costs and benefits;

WHEREAS, San Diego City Council acknowledges the privacy rights of its individual citizens, it also recognizes that surveillance technology may be a valuable tool to support community safety and investigation and prosecution of crimes; and

WHEREAS, San Diego Police Department is accountable to this municipality; responsible for its public safety while granted limited resources; and charged with a mission to serve and protect its residents, rather than to monitor, harass, or intimidate them;

WHEREAS, the City Council finds that surveillance technology includes not just technology capable of accessing non-public places or information (such as wiretaps) but also may include technology which aggregates publicly available information, because such information, in the aggregate or when pieced together with other information, has the potential to reveal a wealth of detail about a person's familial, political, professional, religious, or sexual associations; and awareness that the Government may be watching chills associational and expressive freedoms; and awareness that social control can operate through behavioral data targeting rather than privacy violations.

WHEREAS, we recognize the historical use of surveillance data — both by design or in ways unintended by policy — to intimidate and oppress certain 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 no decisions relating to the City's use of 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 California and United States Constitutions; and

WHEREAS, the City Council finds that any and all decisions regarding if and how the City's surveillance technologies should be funded, acquired, or used should include meaningful public input and that public concern should be given significant weight in policy decisions; and

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 City 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 the public to verify that mandated civil rights and civil liberties safeguards have been strictly adhered to.

NOW, THEREFORE, BE IT ORDAINED by the Council that the City of San Diego adopts the following:

Ordinance which hereby establishes a PRIVACY ADVISORY COMMISSION and establishes processes for ensuring transparency, accountability, and public deliberation informing the City's acquisition and usage of surveillance technology.

SECTION 1. DEFINITIONS. The following definitions apply to this Section:

1. "Commission" means the Privacy Advisory Commission established by this Chapter (hereinafter referred to as the "Privacy Commission" or "Commission").
2. "City" as defined in Section 1 of the Transparent and Responsible Use Of Surveillance Technology Ordinance.
3. "Surveillance" or "surveil" as defined in Section 1 of the Transparent and Responsible Use Of Surveillance Technology Ordinance.
4. "Surveillance technology" as defined in Section 1 of the Transparent and Responsible Use Of Surveillance Technology Ordinance.
5. "Surveillance Impact Report" as defined in Section 1 of the Transparent and Responsible Use Of Surveillance Technology Ordinance.
6. "Surveillance Use Policy" as defined in Section 1 of the Transparent and Responsible Use

Of Surveillance Technology Ordinance.

SECTION 2. ESTABLISHING PRIVACY ADVISORY COMMISSION

Creation of Commission. Pursuant to (Section 43 of the City of San Diego Charter), there is hereby created a San Diego Privacy Advisory Commission.

SECTION 3. DUTIES AND FUNCTIONS

It shall be the duty and function of the Privacy Commission to:

a. Provide advice and technical assistance to the City of San Diego on best practices to protect citizen privacy rights in connection with the City's purchase and use of surveillance equipment and other technology that collects or stores citizen data.

b. Conduct meetings and use other public forums to collect and receive public input on the above subject matter.

c. Draft for City Council consideration, model legislation relevant to the above subject matter, including an Ordinance establishing rules for the City's acquisition and use of Surveillance Technology.

d. Review all new and existing surveillance technology's Surveillance Impact Report and Surveillance Use Policy and make recommendations prior to seeking City Solicitation of Funds and Proposals for Surveillance Technology.

e. Submit annual reports and recommendations to the City Council regarding: (1) the City's use of surveillance equipment, and (2) whether new City surveillance equipment privacy and data retention policies should be developed, or such existing policies be amended.

f. Provide analyses to the City Council of pending federal, state, and local legislation relevant to the City's purchase and/or use of technology that collects, stores, transmits, handles, or processes citizen data.

g. The Privacy Commission shall make reports, findings, and recommendations either to the City Administrator or the City Council, as appropriate. An annual report will be presented in writing to the City Council. The Commission may submit recommendations to the City Council following submission to the City Administrator.

SECTION 4. MEMBERSHIP AND QUORUM

a. The Commission shall consist of nine (9) members, at least six (6) of whom are San Diego residents. Pursuant to Section 43 of the San Diego Charter, Advisory Commissions may be created through ordinance by the City Council. The Mayor shall appoint Commission members through City Council recommendations who will then be confirmed by Council as identified through the Charter. The Mayor is vested with authority to appoint the members of the Commission and if the Mayor does not take such action within forty-five (45) days after the commission is established or a vacancy occurs, the Council shall then make appointments.

b. Five (5) members shall constitute a quorum.

c. Each commission member shall serve as a volunteer without pay.

d. The members shall be appointed to overlapping terms of three (3) years beginning on March 15th of each year and ending on March 15th three years later, or until a successor is appointed and confirmed pursuant to Section 601 of the City Charter. An appointment to fill a vacancy shall be for the unexpired term only. To assure that terms overlap, appointments shall be as follows: three (3) initial members will serve a three-year initial term, three (3) initial members will serve a two-year initial term, and the other three (3) initial members will serve a one-year initial term.

e. In the event an appointment to fill a vacancy has not occurred by the expiration of a member's term, that member may remain in a holdover capacity for up to one year only following the expiration of his or her term or until a replacement is appointed, whichever is earlier.

f. No member of the Privacy Commission shall serve more than three (3) consecutive terms.

g. All members of the Privacy Commission shall be persons who have an interest in privacy rights as demonstrated by work experience, civic participation, and/or political advocacy. No member may be an elected official. Members of the Privacy Commission must represent the following criteria, with no more than 9 members:

1. At least one attorney or legal scholar with expertise in privacy, civil rights, or a representative of an organization with expertise in the same such as but not limited to the American Civil Liberties Union, etc.

2. One auditor or certified public accountant;

3. One hardware, software, or encryption security professional;

4. One member of an organization which focuses on government transparency and openness or an individual, such as a University researcher, with experience working on government transparency and openness.

5. At least four members shall represent equity-focused organizations serving or protecting the rights of communities and groups historically subject to disproportionate surveillance, including diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest.

h. No member may have a financial interest, employment, or policy-making position in any commercial or for profit facility, research center, or other organization that sells data products, surveillance equipment, or otherwise profits from decisions made by the Commission.

SECTION 5. VACANCY AND REMOVAL

a. A vacancy on the Privacy Commission will exist whenever a member dies, resigns, or is removed as per charter, or whenever an appointee fails to be confirmed by the Council within 60 days of appointment. Vacancies shall be filled for any unexpired term provided, however, that if the Mayor does not submit for confirmation a candidate to fill the vacancy within 45 days of the date the vacancy first occurred, the Council may fill the vacancy. If the Mayor does submit for confirmation a candidate to fill a vacancy within the 45-day time frame and the Council does not confirm the candidate, the 45-day period shall commence anew. For purposes of this Section, a seat filled by a holdover appointment will be considered vacant as of the expiration of the holdover's prior term of office.

SECTION 6. COMMISSION GOVERNANCE

a. **OFFICERS AND ELECTIONS**

At the first regular meeting, and subsequently at the first regular meeting of each year, members of the Privacy Commission shall elect a chairperson and a vice chairperson.

b. MEETINGS AND VOTING

The Privacy Commission shall meet at an established regular interval, day of the week,

time, and location suitable for its purpose. Such meetings shall be designated regular meetings. Other meetings scheduled for a time or place other than the regular day, time and location shall be designated special meetings. Written notice of special meetings shall be provided to the Privacy Commission members and all meetings of the Commission shall comport with the Ralph M. Brown Act and the City's Sunshine Act (Chapter 2.2 of San Diego Municipal Code).

The Privacy Commission shall, in consultation with the City Administrator, establish bylaws, rules and procedures for the conduct of its business by a majority vote of the members present. Voting shall be required for the adoption of any motion or resolution.

Any action by the Commission shall be approved by a majority of members present provided a quorum exists.

c. STAFF

Staff assistance may be provided to the Privacy Commission as determined by the City Administrator pursuant to his or her authority under the Charter to administer all affairs of the City under his or her jurisdiction.

SECTION 7 SEVERABILITY

If any section, subsection, sentence, clause or phrase of this Ordinance is for any reason held to be invalid or unconstitutional by decision of any court of competent jurisdiction, such decision shall not affect the validity of the remaining portions of the Chapter. The City Council hereby declares that it would have passed this Ordinance and each section, subsection, clause, or phrase thereof irrespective of the fact that one or more other sections, subsections, clauses, or phrases may be declared invalid or unconstitutional.

SECTION 8 EFFECTIVE DATE

This ordinance shall become effective immediately on final adoption if it receives five or more affirmative votes; otherwise it shall become effective upon the seventh day after final adoption.