ORDINANCE

CITY OF NEW ORLEANS

CITY HALL: June 18, 2020

CALENDAR NO. 33,021

NO. _____ MAYOR COUNCIL SERIES

BY: COUNCILMEMBER WILLIAMS

AN ORDINANCE to amend and reordain Sections 159-1, 159-2, 159-3, 159-4, 159-5, 159-6, 159-7, 159-8, and 159-9 of the Code of the City of New Orleans, to create regulations pertaining to the City's use of surveillance technology, to ban the use of certain technology; to provide for an approval process and Council oversight of the use of surveillance technology; to limit the collection, use and sharing of personal data; to mandate annual surveillance reporting; and otherwise to provide with respect thereto.

WHEREAS, the Council of the City of New Orleans ("City Council") seeks to protect the privacy and human dignity of each individual present in the City; and

WHEREAS, the City Council finds that unchecked surveillance and data collection, governmental or not, can deprive individuals of privacy, impinge on important freedoms, dampen human flourishing, chill the exercise of constitutionally protected free speech, and harm society as a whole; and

WHEREAS, the City Council seeks to protect all its residents and visitors, regardless of immigration status or other trait, and especially members of historically marginalized groups; and

WHEREAS, the City Council recognizes that facial recognition and other surveillance technology is already being used to target and criminalize marginalized groups globally; and

WHEREAS, other U.S. cities, including San Francisco, have already banned the use of facial recognition software by police and other government agencies due to serious concerns of misuse and abuse; and

WHEREAS, the City Council finds that many of the databases to which surveillance technology is applied are plagued by racial and other biases, which generate copycat biases in surveillance data; and

WHEREAS, the City Council believes that debate over whether to use or acquire surveillance technology should occur in a public setting; and

WHEREAS, the City Council finds that if surveillance technology is approved, there must be continued oversight and periodic evaluation to ensure appropriate safeguards are adhered to and that the technology's benefits outweigh its financial and societal costs.

SECTION 1. THE COUNCIL OF THE CITY OF NEW ORLEANS HEREBY ORDAINS, That Sections 159-1, of the Code of the City of New Orleans are hereby reordained to read as follows:

"Section 159-1. – Definitions.

The following words, terms, and phrases, when used in this chapter, shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

Annual Surveillance Report means a written report concerning any specifically defined surveillance technology. An Annual Surveillance Report consists of the following:

1. An updated Surveillance Impact Report with data from the previous year;
2. Information about how often the surveillance technology was used, where it was used, and by which agency or department the technology was used. It should also include the

demographics of the surveillance technology targets, including but not limited to race or ethnicity, gender, and socioeconomic status;

3. Whether and how often data acquired using the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, and justification for the disclosure;

4. All data in the report must be available in a raw and unaggregated form, such as comma separated values (CSV), or otherwise accessible through an online portal.

Automatic license plate reader means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

Automated decision systems are technical systems that aim to aid or replace human decision making.

Cellular communications interception technology, or *cell site simulator* (also known as "Stingrays" or "IMSI Catchers") means any device that intercepts mobile telephony calling information or content, including an international mobile subscriber identity catcher or other virtual base transceiver station that masquerades as a cellular station and logs mobile telephony calling information.

Characteristic tracking system means any software or system capable of tracking people and/or objects based on characteristics such as color, size, shape, age, weight, speed, path, clothing, accessories, vehicle make or model, or any other trait that can be used for tracking purposes, including BriefCam and similar software.

City entity or *city* means any department, agency, attached board or commission of the City of New Orleans.

City official shall mean any person or entity acting on behalf of the City, including any employee, officer, or authorized agent of the City of New Orleans.

Face surveillance or *facial recognition* means an automated or semi-automated process that assists in identifying an individual, capturing information about an individual based on the physical characteristics of an individual's face.

Face surveillance system means any computer software or application that performs face surveillance.

Surveillance Impact Report means a written report concerning a specifically defined surveillance technology, which consists of the following:

1. When completed as part of the initial approval process for new technology, projected information regarding use of the technology;
2. Information describing the surveillance technology, including product descriptions from manufacturers, updated as manufacturers release software updates or other patches that enable new functionalities for existing tools;
3. Information, such as crime statistics, to help community members assess whether the surveillance technology has been or will be effective at achieving its identified purpose;
4. Total annual costs for the surveillance technology, including maintenance and personnel required for use;
5. If applicable, the general location(s) where it may be deployed or has been deployed;
6. An assessment identifying any potential or realized impacts on privacy and civil liberties, as well as plans to safeguard the rights of the public;

7. All data in the report must be available in a raw form, such as CSV, or accessible through an online portal.

Surveillance technology means 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: cell site simulators or "Stingrays"; automatic license plate readers; gunshot detection and location hardware and services, such as ShotSpotter; biometric surveillance technology, including facial, voice, and gait-recognition software and databases; software designed to monitor social media services; software designed to forecast criminal activity or criminality; electronic toll readers; mobile DNA capture technology; video and audio monitoring or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; x-ray vans; radio-frequency identification (RFID) scanners; passive scanners of radio networks; long-range Bluetooth and other wireless-scanning devices; surveillance-capable light bulbs or light fixtures; through-the-wall radar or similar imaging technology; tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network; and software designed to integrate or analyze data from surveillance technology, including target tracking and predictive policing software.
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 above: routine office hardware, such as televisions, computers, and printers, that is in widespread City use and will not be used for any surveillance or surveillance-related functions; Parking Ticket Devices (PTDs); manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; 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 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.

Surveillance Use Policy means a publicly accessible policy for use of surveillance technology which, at a minimum, specifies the following:

1. Purpose: The specific purpose(s) that the surveillance technology is intended to advance.
2. Authorized Use: The uses and capabilities for which the City entity seeks authorization; procedural rules and processes that would govern each authorized use; the uses that would be prohibited; and the methods and circumstances in which data collected, captured, recorded, or intercepted by the surveillance technology would be analyzed and reviewed.
3. Data Collection: The types of information that can be collected by the surveillance technology; the types of data that could be inadvertently collected through the proposed authorized uses of the surveillance technology, and measures the City entity will take to

minimize such inadvertent collection; and the City entity's plan to expeditiously identify and delete inadvertently collected information if permitted by law.

4. Data Access: The individuals or class of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.
5. Data Protection: The safeguards that protect information from unauthorized access, including encryption and access-control mechanisms.
6. 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 needed to further the proposed authorized use(s) of the surveillance technology; the process by which the information will be deleted after that period lapses; and the specific conditions that must be met to retain information beyond that period.
7. Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.
8. Third Party Data Sharing: Whether and how other City or non-City entities can access or use the information, including any required justification or standards for such, and any obligations imposed on the recipient of the information.
9. Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.
10. Auditing and Oversight: The mechanisms to ensure compliance with the Surveillance Use Policy.
11. Functionality: Information describing the surveillance technology and how it works, including product descriptions from manufacturers.
12. Location: The location(s) it may be deployed.

13. Funding: Intended and acceptable funding methods for this surveillance.

Surveillance Use Request means the formal request a City entity submits seeking authorization to use surveillance technology or to permit a third party to use surveillance technology under Section 159-3. It consists of a Surveillance Use Policy and Surveillance Impact Report.

Section 159-2. – Prohibited Surveillance Technology.

No City official or city entity shall obtain, retain, access, use, or authorize a third party to use:

1. Any face surveillance system;
2. Any automatic license plate reader system (ALPR);
    a. An exception is granted for any ALPR that is active on the date this ordinance is passed. Any ALPR physically installed, but which has not been used for enforcement in the 30 day period prior to this ordinance being passed is considered inactive.
    b. Existing fixed ALPRs may only be used at the location they are installed on the date this ordinance is passed. Existing mobile ALPRs may be relocated. No form of ALPR may be replaced, and no new ALPRs may be procured. Existing ALPRs may not be updated or upgraded other than for necessary security patches.
3. Cell-site simulators;
4. Characteristic tracking software;
    a. An exemption is made for any software that has been purchased at the time this ordinance passes. This software can continue to be used normally. It may receive security updates and free software upgrades.
    b. No new features with substantially enhanced capabilities are permitted.

5. Any information obtained from a surveillance system prohibited in this Section.

Section 159-3. – Council Approval of Surveillance Technology.

(a) A City entity must follow the procedures set forth in Section 2-1000 of the Code of the City of New Orleans to submit and obtain City Council approval of a Surveillance Use Request prior to any of the following actions:

1. Acquiring new surveillance technology;
2. Using new surveillance technology, or using existing surveillance technology for a purpose, in a manner, or in a location not previously approved by the Council in accordance with this Chapter, including the sharing of data obtained through the surveillance technology; or
3. Soliciting proposals for, or entering into an agreement with, a non-City entity to acquire, share, or otherwise use surveillance technology or the information it provides.

(b) The Council shall not approve an action enumerated in subsection (a) unless it finds that:

1. The benefits to the community outweigh the costs;
2. The proposal sufficiently protects civil liberties; and
3. The uses and deployments of the surveillance technology will not have a disparate impact on any protected group.

(c) In no event shall the City Council approve use of those surveillance technologies explicitly prohibited under Section 159-2, except as otherwise delineated within that Section.

(d) Each City entity possessing or using surveillance technology, or authorizing a 3rd party to use such surveillance technology, prior to the effective date of this ordinance shall initiate a proposed Surveillance Use Request no later than 180 days following the effective date of

this ordinance for review and approval by Council. If Council approval has not occurred within 365 days of the effective date of this ordinance, the City entity shall immediately cease its use of, or authorization for 3rd party use of, the surveillance technology.

(e) The duration of approval under this section is three (3) years. After this period, a City entity seeking continued use of a Surveillance Technology must submit a new Surveillance Use Request pursuant to this section.

Section 159-4. – Data Sharing and Protection.

(a) Disclosure and rectification: Individuals and organizations may request any City entity disclose what information about them is available in a City database or information system, or any third party database authorized by the City. Further requests can be made to have errors in the data corrected or removed as permitted by law. Requests shall be honored by the City entity within thirty (30) days unless extenuating circumstances necessitate a reasonable extension.

(b) Status data collection ban: The City shall not inquire or collect data regarding any person's immigration status except as required by law or otherwise necessary in order to relay complaints on behalf of such person; determine eligibility for City employment; determine eligibility for a public benefit or program; or otherwise connect such person to supportive services.

(c) Confidential data sharing ban: No employee of the City of New Orleans or a City entity shall disclose to any person or agency outside City government any of the following sensitive information about an individual that comes into the employee's possession during the course and scope of that employee's work for the City or a City entity, except as required by law or otherwise necessary in order to relay complaints on behalf of such

person; determine eligibility for City employment; determine eligibility for a public benefit or program; or otherwise connect such person to supportive services: social security or individual tax identification number, place and date of birth, status as a recipient of public assistance or crime victim, sexual orientation, health status, physical or mental disability.

(d) At the time confidential data is collected from an individual, the City, or an authorized third party on behalf of the City, must disclose the specific data to be collected and any anticipated uses. This disclosure must be followed with written consent from the individual.

(e) The City is responsible for protecting data it collects, and must maintain policies to protect such data from unauthorized access.

(f) Any department that uses, or authorizes a 3rd party to use, a surveillance technology must designate an employee ("Data Protection Officer") responsible for maintaining its compliance with this Chapter.

(g) The City shall maintain procedures for reviewing, sharing, assessing, and evaluating City automated decision systems, including technologies referred to as artificial intelligence, through the lens of equity, fairness, transparency, and accountability. Individuals must have the option to opt-out of all automated decisions.

(h) The City shall collect only the minimum amount of personal information needed to fulfill a well-defined purpose and in a manner consistent with the context in which it will be used.

Section 159-5. – City Contracting.

(a) A private individual or entity shall not cooperate or participate in federal immigration enforcement activities while under contract or other agreement with a City entity, except as required by law.

(b) The City shall not enter into any contract or other agreement that facilitates the receipt of privately generated and owned surveillance data from, or provision of City generated and owned surveillance data to, a non-governmental entity in exchange for any monetary or any other form of consideration from any source, except as authorized pursuant to this Chapter..

(c) The City shall not enter or approve a contract or other agreement that facilitates the surveillance of attorney-client confidential or privileged conversations, despite any warning that such conversations will be monitored, absent a warrant signed by a judge.

Section 159-6. – Transparency and reporting.

(a) By the end of each fiscal year, beginning in fiscal year 2021, a City entity that uses surveillance technology must submit as an official communication to the City Council an Annual Surveillance Report of each approved surveillance technology use. If the City entity is unable to meet the deadline, the department head shall notify Council in writing of its request for an extension and the reasons for that request. The Council may grant reasonable extensions to comply with this Section.

(b) Upon receipt of the Annual Surveillance Report, the City Council may propose modifications to the current Surveillance Use Policy, or, if any expanded uses not specifically authorized by the Council are deemed unacceptable, rescind authorization of the surveillance technology. In reviewing an Annual Surveillance Report, the City Council shall consider the surveillance technology's costs and benefits in terms of investigating and preventing crime; protecting crime victims and promoting public safety; protecting civil rights and liberties, including privacy, free expression and association; and financial costs to the City.

Section 159-7. – Consequences of violation.

Violations of this Ordinance by a City employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements.

Section 159-8. – Severability.

The provisions of this Ordinance are severable. If any part or provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, 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 159-9. – Effective Date.

This ordinance shall take effect on August 1, 2020."

ADOPTED BY THE COUNCIL OF THE CITY OF NEW ORLEANS _____

_____
PRESIDENT OF THE COUNCIL

DELIVERED TO THE MAYOR ON _____

APPROVED:
DISAPPROVED: _____

_____
MAYOR

RETURNED BY THE MAYOR ON _____ AT _____

_____
CLERK OF COUNCIL

ROLL CALL VOTE:
YEAS:
NAYS:
ABSENT:
RECUSED: