Calendar No. (Rev)
(Exp)

Name David Barnes Ext. 5214
Person responsible for routing

CHECK SHEET TO BE USED FOR CLEARING ORDINANCES, MOTIONS, AND RESOLUTIONS BEFORE SUBMISSION TO COUNCIL CLERK

The originating agency shall attach a copy of each proposed ordinance, motion, or resolution to the check sheet for processing in the sequence indicated after preparing a synopsis. The detailed memorandum of explanation shall also be attached to this check sheet.

SYNOPSIS OF DOCUMENT: Proposed ordinance to update Section 147 of the Municipal Code to allow for NOPD and RTCC use of certain surveillance technologies to assist with NOPD investigations and to ensure the swift apprehension of known wanted subjects and prevent imminent injury or death.

1. _____
Department Head
2. _____
Department of Law
3. _____
Chief Administrative Officer
4. _____
Director of Council Relations
5. _____
Initials of Sponsoring Council Member

COUNCIL ACTION

Council Members Present: _____

Absent: _____

AMENDMENTS:

FINAL ADOPTION:

MOVED: _____
2ND: _____
YEAS: _____
NAYS: _____
ABSENT: _____
RECUSED: _____

7. _____
Reviewed by the Chief Administrative Officer after adoption by the City Council and prior to the Mayor's signature.

REF. POLICY MEMORANDUM NO. 3

LEGISLATIVE SUMMARY

TO ACCOMPANY ORDINANCES

BEFORE SUBMISSION TO CLERK OF COUNCIL

Requesting Department or Agency: New Orleans Police Department

Name of Contact Person: David Barnes

Telephone Number: 504-220-6713

Email Address: dabarnes@nola.gov

Initials of Sponsoring Councilmember(s): _____

DETAILED SYNOPSIS OF THE ORDINANCE

Please generally describe the purpose, intent, and effect of the proposed ordinance.

The intent of this proposed ordinance is to allow for the responsible use of certain technologies by NOPD and the New Orleans Real Time Crime Center to assist with the investigation and apprehension of criminal offenders. Technological advances provide for a more robust use of certain technologies with additional safeguards in place to ensure responsible, accountable, and transparent use of the technology. The proposed ordinance also provides for written agreements, reporting requirements, and limitations for any third-parties that agree to assist the NOPD or RTCC with using the technology.

LEGISLATIVE SUMMARY

If the Ordinance is to effectuate a contract, CEA, or other similar agreement (hereafter contract), please provide the following additional information.

☑ **If this section is not applicable, please check this box.**

The parties involved:

The obligations, expectations, and deliverables of the parties involved:

Any fiscal implications for the City with the contract:

The public purpose and need for the contract:

The duration of the contract:

LEGISLATIVE SUMMARY

If the Ordinance is to effectuate an amendment to the Codes of the City of New Orleans, please provide the following additional information.

☐ **If this section is not applicable, please check this box.**

The existing provision(s) of the Code being proposed for amendment:
Additions and modifications to Section 147

The general content/requirements of the existing Code provision:
The existing section includes provisions related to prohibited surveillance technology.

How the proposed ordinance will alter the existing Code provision(s):
The proposed ordinance would allow exceptions for NOPD and the RTCC's use of face surveillance systems and characteristic tracking systems to assist with with the investigation and apprehension of offenses as defined in proposed changes.

Why these changes are needed:
These changes are intended to promote the thoroughness and quality of NOPD investigations by allowing additional investigative tools and to ensure the swift apprehension of known wanted subjects and prevent imminent injury or death.

REQUESTED ADOPTION DATE: _____

Reference: Council Rule 41 & City Code Section 2-813

ORDINANCE

CITY OF NEW ORLEANS

CITY HALL: June 12, 2025

CALENDAR NO. 35,137

NO. _____ MAYOR COUNCIL SERIES

BY: COUNCILMEMBERS THOMAS AND GREEN (BY REQUEST)

AN ORDINANCE to amend and reordain Sections 147-1, 147-2, 147-3, and 147-4 of the Code of the City of New Orleans regarding the use of surveillance technologies; and otherwise to provide with respect thereto.

WHEREAS, facial recognition technology and characteristic tracking systems are critical tools for law enforcement in the identification and apprehension of suspected criminals; and

WHEREAS, had they been available to law enforcement, these tools could have proven invaluable in the expeditious identification and apprehension of the inmates who recently escaped from the Orleans Justice Center, as well as assisted law enforcement with the expedited investigation of terrorist attacks, like the Bourbon Street event on January 1, 2025, to prevent further loss of life; and

WHEREAS, although powerful law enforcement tools, oversight and restrictions are critical to ensure the appropriate use of such surveillance technology; **NOW THEREFORE**

SECTION 1. THE COUNCIL OF THE CITY OF NEW ORLEANS HEREBY ORDAINS, That Sections 147-1, 147-2, 147-3, and 147-4 of the Code of the City of New Orleans, Louisiana are hereby amended to read as follows:

"Chapter 147 – SURVEILLANCE TECHNOLOGY AND DATA PROTECTION

Sec. 147-1. – 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:

Automated decision systems (also known as "ADS") include any software, system, or process that aims to automate, aid, or replace human decision making. Automated decision systems can include both tools that analyze datasets to generate scores, predictions, classifications, or some recommended actions(s) that are used by agencies to make decisions that impact human welfare and the set of processes involved in implementing those tools.

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.

Facial recognition means an automated or semi-automated process that assists in identifying, locating, or verifying the identity of an individual, or capturing information about an individual based on the physical characteristics of an individual's face.

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

Predictive policing technology means the usage of predictive analytics software in law enforcement to predict information or trends about criminality, including but not limited to the perpetrator(s), victim(s), locations or frequency of future crime. It does not include, for example, software used to collect or display historic crime statistics for informational purposes.

Prohibited surveillance technology means (i) facial recognition technology; (ii) cellular communications interception technology or cell site simulator; (iii) characteristic tracking system; or (iv) predictive policing technology.

Real Time Crime Center (RTCC) means the facility managed and operated by the mayor's office of homeland security and emergency preparedness that supports all city public safety agencies using advanced technology.

Surveillance means the act of observing or analyzing the movements, behavior, or actions of identifiable individuals.

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 identifiable individual or group.

(1) "Surveillance technology" includes but is not limited to: cell site simulators; automatic license plate readers; gunshot detection and location hardware and services; 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 used to gain unauthorized access to a computer 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-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; city databases not intended to store or compile surveillance data; and manually-operated technological devices used primarily for internal city communications and not designed to surreptitiously collect surveillance data, such as radios and email systems.

Sec. 147-2. – Prohibited surveillance technology.

(a) Except as otherwise permitted in this section, no city department or agency shall:

(1) Obtain, retain, possess, access, sell, or use any prohibited surveillance technology or information derived from a prohibited surveillance technology;

(2) Enter into an agreement with any third party for the purpose of obtaining, retaining, possessing accessing, selling, or using, on the public right-of-way or on the city's behalf, a prohibited surveillance technology; or

(3) Issue any permit or enter into any other agreement that authorizes any third party, on the public right-of-way or on the city's behalf, to obtain, retain, possess, access, sell,

or use a prohibited surveillance technology or information derived from a prohibited surveillance technology.

(b) Use of any surveillance technology pursuant to this section shall comply with the rules and regulations outlined in the police department policy manual. Evidence obtained solely from the use of any surveillance technology shall not be sufficient to establish probable cause for the purpose of effectuating an arrest.

(c) The police department may use cell-site simulator technology for the following purposes:

(1) To assist in locating a known suspect of a crime enumerated in paragraph (d) below, for which an arrest warrant has been issued and only when the use of such technology is obtained pursuant to a search warrant signed by a neutral and detached judge or magistrate commissioner; or

(2) To assist in locating a missing individual when there is a reasonable belief that the missing individual is in imminent danger of death or serious bodily injury.

(d) The police department or the Real Time Crime Center may use facial recognition technology or information derived therefrom in the investigation of a missing person, and in the investigation of the following crimes:

(1) Solicitation for murder.

(2) First degree murder.

(3) Second degree murder.

(4) Manslaughter.

(5) Aggravated battery.

(6) Second degree battery.

(7) Aggravated assault.

(8) Aggravated or first degree rape.

(9) Forcible or second degree rape.

(10) Simple or third degree rape.

(11) Sexual battery.

(12) Second degree sexual battery.

(13) Aggravated kidnapping.

(14) Second degree kidnapping.

(15) Simple kidnapping.

(16) Aggravated or simple arson.

(17) Aggravated criminal damage to property.

(18) Aggravated or simple burglary.

(19) Armed robbery.

(20) First degree robbery.

(21) Simple robbery.

(22) False imprisonment; offender armed with dangerous weapon.

(23) Assault by drive-by shooting.

(24) Aggravated crime against nature.

(25) Carjacking.

(26) Terrorism.

(27) Aggravated second degree battery.

(28) Aggravated assault upon a peace officer.

(29) Aggravated assault with a firearm.

(30) Armed robbery; use of firearm; additional penalty.

(31) Second degree robbery.

(32) Disarming of a peace officer.

(33) Stalking.

(34) Second degree cruelty to juveniles.

(35) Aggravated flight from an officer.

(36) Battery of a police officer.

(37) Trafficking of children for sexual purposes.

(38) Human trafficking.

(39) Home invasion.

(40) Purse snatching.

(41) Domestic abuse aggravated assault.

(42) Vehicular homicide, when the operator's blood alcohol concentration exceeds 0.20 percent by weight based on grams of alcohol per 100 cubic centimeters of blood.

(43) Aggravated assault upon a dating partner.

(44) Domestic abuse battery punishable under R.S. 14:35.3(L), (M)(2), (N), (O), or (P).

(45) Battery of a dating partner punishable under R.S. 14:34.9(L), (M)(2), (N), (O), or (P).

(46) Identity theft.

(47) Illegal distribution, manufacture, or possession with intent to distribute a controlled dangerous substance.

(48) Violation of a protective order if the violation involves any crime enumerated in this paragraph (d) against the person for whose benefit the protective order is in effect.

(49) Theft, including pickpocketing and theft by fraud, within the following boundaries: the Mississippi River, the center line of Canal Street, the rear property line of the properties fronting on the lake side of North Rampart Street, the rear property line of the properties fronting on the downriver side of Esplanade Avenue to the Mississippi River.

(50) The attempt of any crime enumerated this paragraph (d).

(e) Facial recognition technology or any information derived therefrom shall not be used:

(1) As a surveillance tool, except as provided in this section;

(2) To investigate a violation or attempted violation of any law criminalizing (i) abortion, or the provision thereof by a licensed physician, or (ii) any consensual sexual act between persons of the age of majority, including without limitation any law purporting to criminalize sexual contact between same-sex partners; or

(3) To identify or locate an individual for the sole purpose of determining someone's immigration status or for immigration enforcement.

(f) The police department or RTCC may use facial recognition and characteristic tracking technologies or information derived therefrom under the following circumstances; provided, however, that the source of the technology and the reasons for the request to use the technology must be documented in a police report:

(1) To locate an individual for which a valid arrest warrant exists ordering the apprehension of the individual;

(2) To locate an individual for whom there is reasonable articulable suspicion the individual may cause serious bodily injury or death;

(3) To investigate any of the crimes listed in paragraph (d) above, provided that the use of such surveillance technology is approved by the appropriate police department supervisor and in accordance with the rules and regulations outlined in the police department policy manual; or

(4) To locate a missing individual when there is a reasonable belief that the missing individual is in imminent danger of death or serious bodily injury.

(g) The police department, with assistance from the RTCC, and any third party as required by section 147-4, shall submit a report regarding the use of surveillance technologies in

accordance with this section to the clerk of council for receipt on the consent agenda of the council's first regular meeting scheduled for the months of January, April, July, and September, with copy to the chairperson of the council's criminal justice committee in advance of the committee's quarterly meeting convened pursuant to section 2-61. The report shall be submitted in comma-separated value or similar spreadsheet format and shall include the following information for the preceding calendar quarter:

(1) The total number of requests for the use of facial recognition technology.

(2) The following information for each request:

(i) The requesting officer's name and employee ID number;

(ii) The enumerated crime(s) justifying the request;

(iii) The age, gender and race of the individual identified by the technology;

(iv) The associated police department item number(s);

(v) Whether the use of the technology resulted in a match; and

(vi) Whether the use of the technology resulted in an arrest or criminal charge.

(3) The following information regarding any surveillance technology used by any city department or agency, or by any third party pursuant to written agreement:

(i) The manufacturer, name, and version of any software used;

(ii) Statistical data and any reports regarding the accuracy and efficiency of any software used; and

(iii) The source of any databases or information which is used by the technology to provide identifications or solutions.

(4) Results of the internal audit conducted pursuant to section 147-3.

Sec. 147-3. – Data sharing and protection.

(a) Status data collection ban: The city shall not inquire or collect data regarding any person's immigration status, including place of birth, except in the event of an active federal criminal investigation or when otherwise necessary to relay complaints on behalf of such person; determine eligibility for city employment; determine eligibility for a public benefit or program; or connect such person to supportive services.

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

(c) Any department that uses, or authorizes a third-party to use, a surveillance technology must designate an employee ("data protection officer") responsible for maintaining its compliance with this chapter.

(d) 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. Wherever decisions are made based on the identity of an individual, rather than based on patterns in the general population, such as air traffic control, individuals must have the option to opt out of automated decisions.

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

(f) Data obtained from facial recognition technology, including images and videos, shall not be retained for more than 30 days, unless as part of an active and ongoing investigation, or as otherwise required by law.

(g) The police department shall design and implement an internal auditing procedure or process that ensures department personnel adherence to the provisions of this chapter. The department shall conduct such audit at least quarterly, the results of which shall be included in the quarterly report submitted to the council in accordance with this chapter.

Sec. 147-4. – City contracting.

(a) The city shall not enter into any contract or other agreement that facilitates the receipt of privately generated and owned surveillance technology data from, or provision of city generated and owned surveillance data to, a non-governmental entity in exchange for any monetary donation, in-kind or any other form of consideration from any source, without first providing public notice and an opportunity for public comment.

(b) The city shall not accept or obtain from any non-governmental entity any privately generated and owned surveillance technology data unless pursuant to a written contract or agreement, the terms of which shall require the non-governmental entity to submit quarterly reports, as required in section 147-2, and shall provide that the failure to comply with such reporting constitutes cause for termination of the agreement.

(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.

(d) The city shall not enter into any contract or other agreement for data or information captured by surveillance technology shall be in writing and mandate compliance with the reporting requirements provided herein. Failure to comply with the requirements of this section shall immediately render any agreement with the non-compliant third party null and void."

SECTION 2. That the police department shall review and report on the effectiveness of this ordinance and the use of surveillance technology within the City to the Council's Criminal Justice Committee not later than one year following the adoption of this ordinance.

SECTION 3. That the Clerk of Council shall provide a certified copy of this ordinance to the Chief Administrative Officer, Gilbert Montano, Police Department Superintendent, Anne Kirkpatrick, and Director of the Office of Homeland Security and Emergency Preparedness, Collin Arnold.

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** _____

_____
ASSISTANT CLERK OF COUNCIL

ROLL CALL VOTE:
YEAS:

NAYS:

ABSENT:

RECUSED:

ENGROSSED VERSION

"Chapter 147 – SURVEILLANCE TECHNOLOGY AND DATA PROTECTION

Sec. 147-1. – 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:

Automated decision systems (also known as "ADS") include any software, system, or process that aims to automate, aid, or replace human decision making. Automated decision systems can include both tools that analyze datasets to generate scores, predictions, classifications, or some recommended actions(s) that are used by agencies to make decisions that impact human welfare and the set of processes involved in implementing those tools.

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*~~ ***Facial*** *recognition* means an automated or semi-automated process that assists in identifying**, locating, or verifying the identity of** an individual, **or** capturing information about an individual based on the physical characteristics of an individual's face.

Face ***or facial*** *surveillance system* means any computer software or application that performs ~~face surveillance.~~ **facial recognition.**

Predictive policing technology means the usage of predictive analytics software in law enforcement to predict information or trends about criminality, including but not limited to the perpetrator(s), victim(s), locations or frequency of future crime. It does not include, for example, software used to collect or display historic crime statistics for informational purposes.

Prohibited surveillance technology **means (i) facial recognition technology; (ii) cellular communications interception technology or cell site simulator; (iii) characteristic tracking system; or (iv) predictive policing technology.**

Real Time Crime Center (RTCC) **means the facility managed and operated by the mayor's office of homeland security and emergency preparedness that supports all city public safety agencies using advanced technology.**

Surveillance means the act of observing or analyzing the movements, behavior, or actions of identifiable individuals.

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 identifiable individual or group.

(1) "Surveillance technology" includes but is not limited to: cell site simulators; automatic license plate readers; gunshot detection and location hardware and services; 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 used to gain unauthorized access to a computer 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-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; city databases not intended to store or compile surveillance data; and manually-operated technological devices used primarily for internal city communications and not designed to surreptitiously collect surveillance data, such as radios and email systems.

Sec. 147-2. – Prohibited surveillance technology.

(a) **Except as otherwise permitted in this section,** ~~No~~ **no** city ~~official~~ **department** or ~~city entity~~ **agency** shall:

(1) Obtain, retain, possess, access, sell, or use any prohibited surveillance technology or information derived from a prohibited surveillance technology;

(2) Enter into an agreement with any third party for the purpose of obtaining, retaining, possessing accessing, selling, or using, on the public right-of-way or on the city's behalf, a prohibited surveillance technology; or

(3) Issue any permit or enter into any other agreement that authorizes any third party, on the public right-of-way or on the city's behalf, to obtain, retain, possess, access, sell, or use a prohibited surveillance technology or information derived from a prohibited surveillance technology.

(b) **Use of any surveillance technology pursuant to this section shall comply with the rules and regulations outlined in the police department policy manual. Evidence obtained solely from the use of any surveillance technology shall not be sufficient to establish probably cause for the purpose of effectuating an arrest.** ~~Except as otherwise provided in subsections (c), (d), (e), (f), (g) or (h), the following surveillance technologies are prohibited pursuant to subsection (a):~~

~~(1) Any face surveillance system;~~
~~(2) Cell-site simulator;~~
~~(3) Characteristic tracking system; or~~
~~(4) Predictive policing technology.~~

(c) ~~Nothing in this section shall prohibit the New Orleans Police Department ("NOPD") from using evidence relating to the authorized investigation of a specific crime that may have been generated from a face surveillance or characteristic tracking system, so long as such evidence was not generated by, with the knowledge of, or at the request of the NPPD [NOPD].~~ **The police department may use cell-site simulator technology for the following purposes:**

(1) To assist in locating a known suspect of a crime enumerated in paragraph (d) below, for which an arrest warrant has been issued and only when the use of such technology is obtained pursuant to a search warrant signed by a neutral and detached judge or magistrate commissioner; or

(2) To assist in locating a missing individual when there is a reasonable belief that the missing individual is in imminent danger of death or serious bodily injury.

(d) **The police department or the Real Time Crime Center may use** ~~Nothing in this section shall prohibit NOPD from requesting the use of~~ facial recognition technology **or information derived therefrom in the investigation of a missing person, and** in the investigation of ~~the prior occurrence of~~ the following ~~significant~~ crimes ~~as defined in Louisiana Revised Statute [Title] 14, as of the date of the passage of this section~~.

(1) Solicitation for murder.
(2) First degree murder.
(3) Second degree murder.

(4) Manslaughter.
(5) Aggravated battery.
(6) Second degree battery.
(7) Aggravated assault.
(8) Aggravated or first degree rape.
(9) Forcible or second degree rape.
(10) Simple or third degree rape.
(11) Sexual battery.
(12) Second degree sexual battery.
(13) Aggravated kidnapping.
(14) Second degree kidnapping.
(15) Simple kidnapping.
(16) Aggravated or simple arson.
(17) Aggravated criminal damage to property.
(18) Aggravated or simple burglary.
(19) Armed robbery.
(20) First degree robbery.
(21) Simple robbery.
(22) False imprisonment; offender armed with dangerous weapon.
(23) Assault by drive-by shooting.
(24) Aggravated crime against nature.
(25) Carjacking.
(26) Terrorism.
(27) Aggravated second degree battery.
(28) Aggravated assault upon a peace officer.
(29) Aggravated assault with a firearm.
(30) Armed robbery; use of firearm; additional penalty.
(31) Second degree robbery.
(32) Disarming of a peace officer.
(33) Stalking.
(34) Second degree cruelty to juveniles.
(35) Aggravated flight from an officer.
(36) Battery of a police officer.
(37) Trafficking of children for sexual purposes.
(38) Human trafficking.
(39) Home invasion.
(40) Purse snatching.
(41) Domestic abuse aggravated assault.
(42) Vehicular homicide, when the operator's blood alcohol concentration exceeds 0.20 percent by weight based on grams of alcohol per 100 cubic centimeters of blood.
(43) Aggravated assault upon a dating partner.
(44) Domestic abuse battery punishable under R.S. 14:35.3(L), (M)(2), (N), (O), or (P).

(45) Battery of a dating partner punishable under R.S. 14:34.9(L), (M)(2), (N), (O), or (P).

(46) **Identity theft.**

(47) **Illegal distribution, manufacture, or possession with intent to distribute a controlled dangerous substance.**

(48) Violation of a protective order if the violation involves any crime enumerated ~~above~~ **in this paragraph (d)** against the person for whose benefit the protective order is in effect.

(49) Theft, including pickpocketing and theft by fraud, within the following boundaries: the Mississippi River, the center line of Canal Street, the rear property line of the properties fronting on the lake side of North Rampart Street, the rear property line of the properties fronting on the downriver side of Esplanade Avenue to the Mississippi River.

(50) The attempt of any ~~Any attempted~~ crime ~~of violence~~ enumerated in **this paragraph (d).** ~~subsection (d)(1) (46) above.~~

(e) Facial recognition **technology or any information derived therefrom** shall not be used**:** ~~for the investigation of any crime not enumerated above. This prohibition includes, but is not limited to, the investigation of~~

(1) As a surveillance tool, except as provided in this section;

(2) To investigate a violation or attempted violation of any law criminalizing (~~1~~**i**) abortion or the provision thereof by a licensed physician, ~~and~~ **or** (~~2~~**ii**) any consensual sexual act between persons of the age of majority, including without limitation any law purporting to criminalize sexual contact between same-sex partners~~.~~**; or**

(3) To identify or locate an individual for the sole purpose of determining someone's immigration status or for immigration enforcement.

~~(c) Any officer requesting the use of facial recognition technology shall ensure the request is approved in accordance with current NOPD policy. The council urges the Orleans Parish Criminal District Court to accept a role in receiving information from NOPD on a case by case basis on its use of facial recognition technology and to participate in a working group consisting of members from the following entities:~~

~~(1) New Orleans Police Department~~

~~(2) New Orleans City Council~~

~~The working group will determine the role the court may take or identify an alternative secondary database outside NOPD where information shall be filed.~~

~~Findings of the working group shall be submitted to the council on or before September 30, 2022.~~

~~(f) Evidence obtained from facial recognition alone shall not be sufficient to establish probable cause for the purpose of effectuating an arrest by the NOPD or another law enforcement agency. The source of the image and the underlying reasons for the requested use of facial recognition systems as an investigative lead shall be documented in a police report.~~

~~(g) Facial recognition technology shall not be used as a surveillance tool.~~

~~(h) Nothing in this section shall prohibit an NOPD officer from conducting a criminal investigation using cell-site simulator technology for the following purposes:~~

~~(1) To assist in locating a known suspect of a crime of violence, as defined in section (d) above, for which an arrest warrant has been issued and only when the use of such technology is obtained pursuant to a search warrant signed by a neutral and detached judge or magistrate commissioner; or~~

~~(2) To assist in locating a missing individual when there is a reasonable belief that the missing individual is in imminent danger of death or is in imminent danger of receiving serious bodily injury as defined in R.S. 14:2(C).~~

(f) The police department or RTCC may use facial recognition and characteristic tracking technologies or information derived therefrom under the following circumstances; provided, however, that the source of the technology and the reasons for the request to use the technology must be documented in a police report:

(1) To locate an individual for which a valid arrest warrant exists ordering the apprehension of the individual;

(2) To locate an individual for whom there is reasonable articulable suspicion the individual may cause serious bodily injury or death;

(3) To investigate any of the crimes listed in paragraph (d) above, provided that the use of such surveillance technology is approved by the appropriate police department supervisor and in accordance with the rules and regulations outlined in the police department policy manual; or

(4) To locate a missing individual when there is a reasonable belief that the missing individual is in imminent danger of death or serious bodily injury.

(~~i~~**g**) The **police department,** ~~New Orleans Police Department, acting in conjunction with the Louisiana State Analytical and Fusion Exchange (LA-SAFE)~~ **with assistance from the RTCC, and any third party as required by section 147-4**, shall submit a ~~quarterly~~ report regarding the use of surveillance technologies ~~pursuant to~~ **in accordance with** this section to the clerk of council ~~Clerk of Council~~ **for receipt on the consent agenda of the council's first regular meeting scheduled for the months of January, April, July, and September,** with a copy ~~and~~ to the ~~Chair~~ **chairperson** of the ~~City Council's Criminal Justice Committee~~ **council's criminal justice committee in advance of the committee's quarterly meeting convened pursuant to section 2-61.** ~~to coincide with other required updates from law enforcement bodies transmitted in advance of the quarterly convening of the Criminal Justice Committee per Ordinance Calendar Number 33,724-29063 M.C.S.~~ The report shall be ~~saved and~~ submitted in **comma-separated value** ~~searchable PDF~~ or **similar** spreadsheet format and shall include the following information **for the preceding calendar quarter**:

(1) The total number of requests for the use of facial recognition technology.

(2) ~~For~~ **The following information for** each request:

~~a.~~**(i)** The requesting officer's name and ~~badge~~ **employee ID** number;

~~b.~~**(ii)** The enumerated crime(s) justifying the request;

~~c.~~**(iii)** The age, gender and race of the ~~suspect~~ **individual identified by the technology**;

~~d.~~**(iv)** The ~~accompanying~~ **associated police department** ~~NOPD/Orleans Parish Communication District (OPCD)~~ item numbers~~**(s)**~~,

~~e.~~**(v)** Whether the use of ~~facial recognition~~ **the** technology resulted in a match; and

~~f.~~**(vi)** Whether the use of ~~facial recognition~~ **the** technology resulted in an arrest ~~and/~~or **criminal** charge~~s~~.

(3) The following information regarding any surveillance technology used by any city department or agency, or by any third party pursuant to written agreement:

(i) The manufacturer, name, and version of any software used;

(ii) Statistical data and any reports regarding the accuracy and efficiency of any software used; and

(iii) The source of any databases or information which is used by the technology to provide identifications or solutions.

(4) Results of the internal audit conducted pursuant to section 147-3.

~~(j) Notwithstanding section 147-7, the provisions of section 147-2(d) shall take effect on October 1, 2022.~~

Sec. 147-3. – Data sharing and protection.

(a) Status data collection ban: The city shall not inquire or collect data regarding any person's immigration status, including place of birth, except in the event of an active federal criminal investigation or when otherwise necessary to relay complaints on behalf of such person; determine eligibility for city employment; determine eligibility for a public benefit or program; or connect such person to supportive services.

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

(c) Any department that uses, or authorizes a third-party to use, a surveillance technology must designate an employee ("data protection officer") responsible for maintaining its compliance with this chapter.

(d) 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. Wherever decisions are made based on the identity of an individual, rather than based on patterns in the general population, such as air traffic control, individuals must have the option to opt out of automated decisions.

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

(f) Data obtained from facial recognition technology, including images and videos, shall not be retained for more than 30 days, unless as part of an active and ongoing investigation, or as otherwise required by law.

(g) The police department shall design and implement an internal auditing procedure or process that ensures department personnel adherence to the provisions of this chapter. The department shall conduct such audit at least quarterly, the results of which shall be included in the quarterly report submitted to the council in accordance with this chapter.

Sec. 147-4. – City contracting.

(a) The city shall not enter into any contract or other agreement that facilitates the receipt of privately generated and owned surveillance **technology** data from, or provision of city generated and owned surveillance data to, a non-governmental entity in exchange for any monetary donation, in-kind or any other form of consideration from any source, without first providing public notice and an opportunity for public comment.

(b) **The city shall not accept or obtain from any non-governmental entity any privately generated and owned surveillance technology data unless pursuant to a written contract or agreement, the terms of which shall require the non-governmental entity to submit quarterly reports, as required in section 147-2, and shall provide that the failure to comply with such reporting constitutes cause for termination of the agreement.**

(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.

(d) The city shall not enter into any contract or other agreement for data or information captured by surveillance technology shall be in writing and mandate compliance with the reporting requirements provided herein. Failure to comply with the requirements of this section shall immediately render any agreement with the non-compliant third party null and void."