LAID ON THE TABLE

Submitted by: Chair of the Assembly at the Request of the Mayor
Prepared by: Dept. of Law
For reading: April 11, 2023

ANCHORAGE, ALASKA
AO No. 2023-35 (S)

AN ORDINANCE OF THE ANCHORAGE ASSEMBLY AMENDING ANCHORAGE MUNICIPAL CODE CHAPTER 3.102, *MUNICIPAL USE OF SURVEILLANCE TECHNOLOGIES,* TO BAN THE ACQUISITION, USE, OR ACCESSING OF FACIAL RECOGNITION TECHNOLOGY WITH LIMITED EXCEPTIONS, AND TO REORGANIZE THE CHAPTER.

WHEREAS, facial recognition is a remarkable development that helps law enforcement exonerate the innocent, narrow searches for the guilty, and otherwise maximize limited resources through the rapid comparison of one facial image to many others; and

[~~WHEREAS, Facial Recognition Technology has become increasingly common in society, despite the efficacy of its use still remaining largely unknown; and~~]

WHEREAS, there currently exist no federal or Alaska state law or administrative regulations governing the use of Facial Recognition Technology nor any clearly established guidelines or best practices; and

WHEREAS, the success of facial recognition technologies as an effective tool for law enforcement is dependent upon ensuring that they are properly deployed and used; and

[~~WHEREAS, unlike established forensic scientific evidence techniques, Facial Recognition Technology uniquely lends itself to potential abuse or manipulation as its users can lower "confidence levels" until they get a positive result, leading to even lower accuracy for identification; and~~]

WHEREAS, facial recognition technology is more accurate and advanced than the human eye. According to the National Institute of Standards and Technology (NIST), there are algorithms that can match a photo out of a lineup of over 12 million photos over 99% of the time for all demographics; and

[~~WHEREAS, multiple studies have determined that Facial Recognition Technology disproportionately misidentifies people of color most frequently of all demographics; and~~]

WHEREAS, in general the Facial Recognition Technologies establish a unique identifier for each person with the data collected, often without a person's consent, and as biologically unique information it is inherently private to the individual; and

WHEREAS, an individual's right to privacy is protected by the Fourth Amendment of the U.S. Constitution and is explicitly immortalized in Alaska Constitution Art. 1,

§ 22, known as one of the strongest guarantees of privacy in the country; and

WHEREAS, the Assembly desires to protect the right to privacy by codifying certain restrictions on the use of Facial Recognition Technologies by any municipal department or agency in a manner that's improper, surreptitious, or oversteps an individual's privacy rights; now, therefore,

THE ANCHORAGE ASSEMBLY ORDAINS:

Section 1. Anchorage Municipal Code section 3.102 Municipal Use of Surveillance Technologies hereby amended to read as follows (*the remainder of the section is not affected and therefore not set out)*:

Chapter 3.102 - MUNICIPAL USE OF SURVEILLANCE TECHNOLOGIES

3.102.005. Definitions

Authorized use **means the use of facial recognition technology to (i) help identify an individual when there is a reasonable suspicion the individual has committed a crime; (ii) help identify a crime victim, including a victim of online sexual abuse material; (iii) help identify a person who may be a missing person or witness to criminal activity; (iv) help identify a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or wildlife; (v) help identify an online recruiter of criminal activity, including but not limited to human, weapon, drug, and wildlife trafficking; (vi) help a person who is suffering from a mental or physical disability impairing his ability to communicate and be understood; (vii) help identify a deceased person; (viii) help identify a person who is incapacitated or otherwise unable to identify himself; (ix) help identify a person who is reasonably believed to be a danger to himself or others; (x) help identify an individual lawfully detained; (xi) help mitigate an imminent threat to public safety, a significant threat to life, or a threat to national security, including acts of terrorism; (xii) ensure officer safety as part of the vetting of undercover law enforcement; (xiii) determine whether an individual may have unlawfully obtained one or more state driver's licenses, financial instruments, or other official forms of identification using information that is fictitious or associated with a victim of identity theft; or (xiv) help identify a person who an officer reasonably believes is concealing his true identity and about whom the officer has a reasonable suspicion has committed a crime other than concealing his identity.**

Facial Recognition means an automated or semi-automated process that assists in identifying or verifying an individual, or capturing information about an individual, based upon analysis of the individual's face.

Facial Recognition Technology means **an electronic system or service for conducting an algorithmic comparison of images of a person's facial features for the purpose of identification [~~any computer software or application that performs facial recognition~~]**. ***Facial recognition technology*** **does not include the use of an automated or semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the recording prior to release or disclosure of the recording outside of the law-enforcement agency if the process does not generate or result in the retention of any biometric data or surveillance information.**

Publicly post **means to post on a website that is maintained by the entity or on any other website on which the entity generally posts information and that is available to the public or that clearly describes how the public may access such data.**

Surveillance or *Surveil* means to observe or analyze the movements, behavior, data, or actions of individuals. Individuals include those whose identity can be determined through use of information maintained by the department of motor vehicles either independently or when combined with any other record.

Surveillance Technology means any software, electronic device, system utilizing an electronic device, or similar used, designed, or primarily intended to 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.

UAS/Unmanned aircraft systems means a system that includes the necessary equipment, network, and personnel to control an unmanned aircraft.

UA/Unmanned aircraft means an aircraft that is intended to navigate in the air without an on-board pilot. Also alternatively called a remotely piloted aircraft (RPA), remotely operated vehicle (ROV), or drone.

(AO No. 2018-5, § 1, 2-13-18)

3.102.010 - Restrictions on the use of unmanned aircraft systems by the municipality.

*** *** ***

[B. NO LATER THAN JUNE 1 OF EACH YEAR, THE MAYOR OR A DESIGNEE SHALL TRANSMIT TO THE ASSEMBLY AND CAUSE TO BE PUBLICLY POSTED ON THE MUNICIPAL WEBSITE A REPORT WITH THE ALL FOLLOWING INFORMATION:

1. FOR EACH MUNICIPAL DEPARTMENT AND AGENCY THAT USED A UAS IN THE PRECEDING CALENDAR YEAR:

   a. THE NUMBER OF INSTANCES IN WHICH A UAS WAS USED;

   b. A GENERAL DESCRIPTION OF THE TYPE AND PURPOSE OF EACH USE THAT SUFFICIENTLY EXPLAINS HOW THE USE WAS NOT PROHIBITED BY THIS SECTION, AND, IF APPLICABLE, WHETHER THE USE WAS PURSUANT TO A SEARCH WARRANT, A COURT ORDER, OR A JUDICIALLY RECOGNIZED EXCEPTION TO THE WARRANT REQUIREMENT; AND

   c. ANY NEW POLICY, OR CHANGE IN DEPARTMENT OR AGENCY POLICY, RELATED TO THE USE OF UAS.

2. THE ANNUAL REPORT FROM THE ANCHORAGE POLICE DEPARTMENT SHALL ALSO INCLUDE:

   a. THE NUMBER OF ARRESTS MADE WHERE UAS WAS UTILIZED IN A RELATED INCIDENT RESPONSE OR INVESTIGATION, REGARDLESS OF WHETHER THE INFORMATION GATHERED FROM THE UAS WAS USED TO ESTABLISH PROBABLE CAUSE.

C. DEFINITIONS.

1. UAS/UNMANNED AIRCRAFT SYSTEMS MEANS A SYSTEM THAT INCLUDES THE NECESSARY EQUIPMENT, NETWORK, AND PERSONNEL TO CONTROL AN UNMANNED AIRCRAFT.

2. UA/UNMANNED AIRCRAFT MEANS AN AIRCRAFT THAT IS INTENDED TO NAVIGATE IN THE AIR WITHOUT AN ON-BOARD PILOT. ALSO ALTERNATIVELY CALLED A REMOTELY PILOTED AIRCRAFT (RPA), REMOTELY OPERATED VEHICLE (ROV), OR DRONE.]

(AO No. 2018-5, § 1, 2-13-18)

3.102.020. - Restrictions on the use of facial recognition technology.

A. Notwithstanding any other provision of this chapter except for the exceptions provided in section 3.102.030, it shall be unlawful for the municipality or any municipal staff to obtain, retain, request, access, or use:

1. Facial Recognition Technology; or

2. Information obtained from Facial Recognition Technology.

B. Municipal staff's inadvertent or unintentional receipt, access of, or use of any information obtained from Facial Recognition Technology shall not be a violation of this section, provided that:

1. Municipal staff did not request or solicit the receipt, access of. or use of such information: and

2. Municipal staff logs such receipt, access, or use in its Annual Surveillance Report as referenced by Section 3.102.040. Such report shall not include any personally identifiable information or other information the release of which is prohibited by law.

3.102.030. Exceptions.

A. Nothing in this chapter shall prevent the Municipality from:

1. Acquiring, obtaining, retaining, or accessing facial recognition technology on an electronic device intended for a single user, such as a mobile communication device, cellular phone or tablet, when the facial recognition technology is used solely for the purpose of the user;

2. Acquiring, obtaining, retaining, or accessing social media or communications software or applications intended for communication with the general public that include facial recognition technology, as long as the municipality does not intentionally use the facial recognition technology;

3. Having custody or control of electronic devices that include facial recognition technology when such electronic devices are held by the municipality solely for evidentiary purposes;

4. Acquiring, obtaining, retaining, or accessing facial recognition technology solely for the purpose of using automated or semiautomated redaction software;

5. Complying with the National Child Search Assistance Act, 34 U.S.C. §§ 41307-413087, or other federal statutes requiring cooperation in the search for missing or exploited children; or

6. Participate in, coordinate with, or otherwise be involved with multi-agency law enforcement investigations, working groups or task forces.

B. It shall not be a violation of this chapter for the municipality to acquire, obtain, or retain facial recognition technology when all the following conditions exist:

1. The facial recognition technology is an integrated, off the shelf capability, bundled with software or stored on a product or device;

2. Other functions of the software, product, or device are necessary or beneficial to the performance of municipal functions;

3. The software, product, or device is not acquired for the purpose of performing facial recognition;

4. The facial recognition technology cannot be deleted from the software, product, or device;

5. The municipality does not use the facial recognition technology; and

6. The municipal department, agency or official seeking to acquire the software, product, or device discloses the integrated, off the shelf facial recognition technology that cannot be deleted to the Assembly when seeking to acquire the software, product, or device.

C. Recognizing that changes in technology and circumstances may require additional exceptions to the requirements of this section, the assembly may approve such additional exceptions by resolution, under the following conditions:

1. Any municipal department that requests an exception to the restrictions of section 3.102.020 shall include in its request to the assembly an explanation of the need for an exception, a description of how the technology or information will be used, and a plan for monitoring the technology or information to ensure that its use remains within the approved parameters.

2. The assembly may approve the proposed exception by resolution, with or without revisions and conditions, for a period of no longer than 90 days, if it finds that the exception is consistent with the stated goals of preventing discrimination and promoting privacy, transparency, and the public trust.

3. Upon conclusion of the period of temporary exception, the department shall submit a report of its uses of the technology or information to the assembly. The department may at that time or subsequently request the assembly make the exception permanent by ordinance adding it under section 3.102.030D.

4. A department that has obtained a permanent exception shall submit an annual summary of its uses of the technology or information as part of the Annual Surveillance Report under Section 3.102.040 to the assembly. This summary shall not

include personally identifiable information.

D. Additional permanent exceptions.

1. [~~Reserved.~~] **Anchorage Police Department.**

a. The Anchorage Police Department may use facial recognition technology for authorized uses. A match made through facial recognition technology shall not be included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an arrest warrant but shall be admissible as exculpatory evidence. The Anchorage Police Department shall not (i) use facial recognition technology for tracking the movements of an identified individual in a public space in real time; (ii) create a database of images using a live video feed for the purpose of using facial recognition technology; or (iii) enroll a comparison image in a commercial image repository of a facial recognition technology service provider except pursuant to an authorized use. Following such use as provided in clause (iii), no comparison image may be retained or used further by the service provider except as required for auditing that use or as may be otherwise required by law.

b. The Anchorage Police Department shall publicly post and annually update its policy regarding the use of facial recognition technology before employing such facial recognition technology to investigate a specific criminal incident or citizen welfare situation. The Anchorage Police Department shall not utilize any facial recognition technology until after publication of the department's policy regarding the use of facial recognition technology.

3.102.040. - Reports of municipal use of surveillance technologies required.

A. The purchase and use of any facial recognition technology must be evaluated by the National Institute of Standards and Technology (NIST) as part of the Face Recognition Vendor Test. Any facial recognition technology utilized shall utilize algorithms that have demonstrated (i) an accuracy score of at least 98 percent true positives within one or more datasets relevant to the application in a NIST Face Recognition Vendor Test report and (ii) minimal performance variations across demographics associated with race, skin tone, ethnicity, or

gender. The municipality shall require all approved vendors to annually provide independent assessments and benchmarks offered by NIST to confirm continued compliance with this section.

B. At least 30 days prior to procuring facial recognition technology, any municipal department shall notify the Assembly in writing that such agency intends to procure facial recognition technology.

C. Any municipal department or staff that uses facial recognition technology shall maintain records sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public reporting, and auditing of compliance with such agency's facial recognition technology policies. Such agency shall collect data pertaining to (i) a complete history of each user's queries; (ii) the total number of queries conducted; (iii) the number of queries that resulted in a list of possible candidates; (iv) how many times an examiner offered law enforcement an investigative lead based on his findings; (v) how many cases were closed due to an investigative lead from facial recognition technology; (vi) what types of criminal offenses are being investigated; (vii) the nature of the image repository being compared or queried; (viii) demographic information for the individuals whose images are queried; and (ix) if applicable, any other entities with which the department shared facial recognition data.

D. The Mayor or his designee shall transmit to the Assembly and cause to be publicly posted on the municipal website an annually updated report by June 1 each year to provide information to the public regarding any department's use of facial recognition technology. The report shall include all data required by clauses (ii) through (viii) of subsection C in addition to (i) all instances of unauthorized access of the facial recognition technology, including any unauthorized access by employees of the department; (ii) vendor information, including the specific algorithms employed; and (iii) if applicable, data or links related to third-party testing of such algorithms, including any reference to variations in demographic performance. If any information or data (a) contains an articulable concern for any person's safety; (b) is otherwise prohibited from public disclosure by federal or state statute; or (c) if disclosed, may compromise sensitive criminal justice information, such information or data may be excluded from public disclosure. Nothing herein shall limit disclosure of data collected pursuant to subsection C when such disclosure is related to a writ of habeas corpus. For purposes of this subsection, "sensitive criminal justice information" means information related to (1) a particular ongoing criminal investigation or proceeding, (2) the identity of a confidential source, or (3) law-enforcement

investigative techniques and procedures.

[~~**A. No later than June 1 of each year, the mayor or a designee shall transmit to the assembly and cause to be publicly posted on the municipal website an Annual Surveillance Report with all the following information:**~~

~~**1. For each municipal department and agency that used a UAS in the preceding calendar year:**~~

~~**a. The number of instances in which a UAS was used;**~~

~~**b. A general description of the type and purpose of each instance that sufficiently explains how the use was not prohibited by this chapter, and, if applicable, whether the use was pursuant to a search warrant, a court order, or a judicially recognized exception to the warrant requirement, and the final disposition of evidence resulting from each instance; and**~~

~~**c. Any new policy, or change in department or agency policy, related to the use of UAS or Facial Recognition Technology**~~

~~**2. For each municipal department or agency using Facial Recognition Technology under an exception under section 3.102.030:**~~

~~**a. The number of instances in which Facial Recognition Technology was used or information derived from Facial Recognition Technology was received or used under exceptions in subsections 3.102.030A.4., A.5., A.6., C. and D.;**~~

~~**b. A general description of the type and purpose of each instance that sufficiently explains how the use was not prohibited by this chapter, and, if applicable, whether the use was pursuant to a search warrant, a court order, or a judicially recognized exception to the warrant requirement, and the final disposition of evidence resulting from each instance; and**~~

~~**c. Any new policy, or change in department or agency policy, related to the use of Facial Recognition Technology**~~

~~**3. The annual report shall also include the following information:**~~

~~a. The number of arrests made by APD where UAS was utilized in a related incident response or investigation, regardless of whether the information gathered from the UAS was used to establish probable cause.~~

~~b. The detailed log of every unauthorized receipt, access, or use of Facial Recognition Technology or information derived from Facial Recognition Technology. The log shall denote how the unauthorized access occurred, what corrective steps have been taken, and the final disposition of any evidence or information improperly received.]~~

(AO No. 2018-5, § 1, 2-13-18)

3.102.050. Enforcement.

A. Any municipal employee who violates a provision of this chapter may be subject to discipline in accordance with the municipality's disciplinary policies and procedures and applicable collective bargaining agreements. Violation of this ordinance by any official or employee of the municipal is grounds for suspension or termination. The disciplinary action may require the violator to participate in retraining.

B. Private cause of action.

1. Any violation of this article constitutes an injury and any person so injured may institute proceedings in the Superior Court in a civil action seeking injunctive relief, declaratory relief, damages, and attorney's fees. Any action instituted under this paragraph shall be brought against the municipality. If applicable, such action may also be brought against any third party with whom the municipality contracted or entered into an agreement.

2. Any person who has instituted proceedings under the previous paragraph and is found to have been subjected to face surveillance in violation of this article, or about whom data or information is found to have been obtained, retained, stored, possessed, accessed, used, or collected in violation of this article, shall be entitled to recover actual damages not less than the greater of:

a. $1,000 for each violation of this article; or

b. $10,000.

3. Any prevailing plaintiff in any action brought under this

subsection shall be entitled to the award of costs and reasonable attorney's fees.

Section 2. This ordinance shall be effective immediately upon passage and approval by the Assembly.

PASSED AND APPROVED by the Anchorage Assembly this _____ day of _____, 2023.

Chair _____

ATTEST:

_____
Municipal Clerk

MUNICIPALITY OF ANCHORAGE

Assembly Memorandum

No. AM 279-2023

Meeting Date: April 11, 2023

From: **MAYOR**

Subject: **AO No. 2023-35(S): AN ORDINANCE OF THE ANCHORAGE ASSEMBLY AMENDING ANCHORAGE MUNICIPAL CODE CHAPTER 3.102, *MUNICIPAL USE OF SURVEILLANCE TECHNOLOGIES,* TO BAN THE ACQUISITION, USE, OR ACCESSING OF FACIAL RECOGNITION TECHNOLOGY WITH LIMITED EXCEPTIONS, AND TO REORGANIZE THE CHAPTER.**

This substitute ordinance reflects alternative language proposed by the Anchorage Police Department ("APD"). The Department believes that with the following modifications, a ban of facial recognition technology could be successfully implemented.

- This version adds an exception for APD to use facial recognition technology for certain authorized uses including the identification of individuals suspected of committing a crime, as well as for the protection of victims of a crime, incapacitated individuals, or other individuals under threat of imminent danger.
- This version also proposes alternative language requiring that any municipal department wishing to make use of facial recognition technology use technology that has been evaluated by the National Institute of Standards and Technology.
- Finally, this version provides that any municipal department wishing to make use of facial recognition technology provide the Assembly with thirty days notice. In addition, the Mayor would produce a publicly available annual report providing municipal departments' use of facial recognition technology.

Adoption of this ordinance will have no significant cost to the Municipality, and no financial impact to the private sector is anticipated; therefore, no Summary of Economic Effects is included.

THE ADMINISTRATION RECOMMENDS APPROVAL.

Prepared by:	Department of Law
Concur:	Anne Helzer, Acting Municipal Attorney
Concur:	Kent Kohlhase, Acting Municipal Manager
Respectfully submitted:	Dave Bronson, Mayor