LAID ON THE TABLE

Submitted by: Assembly Members Sweet, Rivera, and Volland
Prepared by: Assembly Counsel's Office
For reading:

ANCHORAGE, ALASKA
AO No. 2023-35(S-1)

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.

(NOTE: in this S-1 version, the markup shows changes from the original AO only, and does not reflect any of the additions or deletions proposed in the S version. Therefore, additions are shown in* **underline and bold, *and deletions indicated by* **[~~brackets, strikethrough, and bold~~].**

WHEREAS, Facial Recognition Technology has become increasingly common in society**, and while it has the possibility to assist law enforcement in its work to keep the public safe under strict regulations, its efficacy and specificity still remain[~~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, Facial Recognition Technology is a quickly evolving form of artificial intelligence and has the potential to be used in the future by various Municipal departments for diverse functions, but is a tool that should be used with a high regard for the privacy rights of both Municipal employees and the general public; 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, 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, the successful use of Facial Recognition Technology as an effective law enforcement tool is dependent on ensuring safeguards for the public and that they are properly deployed and used; 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, new biometric technologies have the ability to enhance the functions of government and its encroachment on our daily lives and must be balanced with appropriate checks-and-balances to ensure the "consent of the governed;" 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

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 any computer software or application that performs facial recognition.

***Real-time* describes the operation or execution of an action or process, by either human or technological means, contemporaneous to an identified event.**

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. **The use facial recognition technology in conjunction with or, as component of, any real-time surveillance or surveillance technology by the municipality or any municipal staff shall be unlawful.**

B. 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.

C.[~~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.

D. Any evidence or information obtained through facial recognition technology, regardless of whether it was obtained lawfully, shall not be included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an arrest warrant.

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. **Specifically, municipal law enforcement may intentionally work with third party agencies using Facial Recognition Technology to identify:**

a. Human remains or suspected missing persons;

b. Suspected victims of human trafficking; or

c. Suspected victims of child abuse or exploitation.

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 **pursuant to a public hearing**, 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.

3.102.040. Reports of municipal use of surveillance technologies required.

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

LAID-ON-THE-TABLE

MUNICIPALITY OF ANCHORAGE

Assembly Memorandum

No. AM - 2023

Meeting Date: April 18, 2023

From: **Members Sweet, Rivera, and Volland**

Subject: **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 version of the AO 2023-35 makes the following substantive changes to the proposed ordinance:

- Whereas statements making clear the intent to thoughtfully and deliberately regulate the uses and potential adoption of facial recognition technology while respecting the public's right to privacy.

- A blanket prohibition on the use of the facial recognition technology to conduct real-time surveillance, regardless of whether the facial recognition technology is approved for use as an exception. It also defines the term "real-time."

- A blanket prohibition on the use of evidence derived from facial recognition technology to establish probable cause necessary for issuance of a search or arrest warrant, regardless of whether the evidence was obtained lawfully or unlawfully.

- Explicit provisions for the use of facial recognition technology through third party agencies to assist law enforcement in identifying missing persons, as well as victims of human trafficking. Generally, investigations into such matters are not done entirely in house by local law enforcement, but in cooperation and coordination with National Center for Missing and Exploited Children and/or the FBI's Human Trafficking Task Forces. While the original text of the proposed ordinance allowed for this kind activities, the authors felt it important to make clear the ordinance is not intended to inhibit these critical investigations.

- Adds to the exception process the requirement of a public hearing when the assembly is considering authorizing by resolution the temporary use or procurement of facial recognition technology for a period of 90 days or

less.

We request your support for the ordinance.

Prepared by: Assembly Counsel's Office

Respectfully submitted: Joey Sweet, Assembly Member
District 5, East Anchorage

Felix Rivera, Assembly Member
District 4, Midtown

Daniel Volland, Assembly member
District 1, North Anchorage