

Submitted by: Assembly Members Sweet, Rivera,
and Volland

Prepared by: Assembly Counsel's Office

For reading:

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

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

6
7 **WHEREAS**, Facial Recognition Technology has become increasingly common in
8 society, despite the efficacy of its use still remaining largely unknown; and
9

10 **WHEREAS**, there currently exist no federal or Alaska state law or administrative
11 regulations governing the use of Facial Recognition Technology nor any clearly
12 established guidelines or best practices; and
13

14 **WHEREAS**, unlike established forensic scientific evidence techniques, Facial
15 Recognition Technology uniquely lends itself to potential abuse or manipulation as
16 its users can lower “confidence levels” until they get a positive result, leading to even
17 lower accuracy for identification; and
18

19 **WHEREAS**, multiple studies have determined that Facial Recognition Technology
20 disproportionately misidentifies people of color most frequently of all demographics;
21 and
22

23 **WHEREAS**, in general the Facial Recognition Technologies establish a unique
24 identifier for each person with the data collected, often without a person’s consent,
25 and as biologically unique information it is inherently private to the individual; and
26

27 **WHEREAS**, an individual’s right to privacy is protected by the Fourth Amendment
28 of the U.S. Constitution and is explicitly immortalized in Alaska Constitution Art. 1,
29 § 22, known as one of the strongest guarantees of privacy in the country; and
30

31 **WHEREAS**, the Assembly desires to protect the right to privacy by codifying certain
32 restrictions on the use of Facial Recognition Technologies by any municipal
33 department or agency in a manner that’s improper, surreptitious, or oversteps an
34 individual’s privacy rights; now, therefore,
35

36 **THE ANCHORAGE ASSEMBLY ORDAINS:**
37

38 **Section 1.** Anchorage Municipal Code section 3.102 Municipal Use of
39 Surveillance Technologies hereby amended to read as follows (*the remainder of the*
40 *section is not affected and therefore not set out*):
41

42 **Chapter 3.102 - MUNICIPAL USE OF SURVEILLANCE TECHNOLOGIES**
43

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, with no noticeable delay.

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:

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50

- 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**

1 municipality or any municipal staff to obtain, retain, request, access,
2 or use:

3
4 1. Facial Recognition Technology; or

5
6 2. Information obtained from Facial Recognition Technology.

7
8 **C.[B].** Municipal staff's inadvertent or unintentional receipt, access of, or use
9 of any information obtained from Facial Recognition Technology shall
10 not be a violation of this section, provided that:

11
12 1. Municipal staff did not request or solicit the receipt, access of,
13 or use of such information: and

14
15 2. Municipal staff logs such receipt, access, or use in its Annual
16 Surveillance Report as referenced by Section 3.102.040. Such
17 report shall not include any personally identifiable information
18 or other information the release of which is prohibited by law.

19
20 **D.** Any evidence or information obtained through facial recognition
21 technology, regardless of whether it was obtained lawfully, shall
22 not be included in an affidavit to establish probable cause for
23 purposes of issuance of a search warrant or an arrest warrant.

24
25 **3.102.030. Exceptions.**

26
27 **A.** Nothing in this chapter shall prevent the Municipality from:

28
29 1. Acquiring, obtaining, retaining, or accessing facial recognition
30 technology on an electronic device intended for a single user,
31 such as a mobile communication device, cellular phone or
32 tablet, when the facial recognition technology is used solely for
33 the purpose of the user;

34
35 2. Acquiring, obtaining, retaining, or accessing social media or
36 communications software or applications intended for
37 communication with the general public that include facial
38 recognition technology, as long as the municipality does not
39 intentionally use the facial recognition technology;

40
41 3. Having custody or control of electronic devices that include
42 facial recognition technology when such electronic devices are
43 held by the municipality solely for evidentiary purposes;

44
45 4. Acquiring, obtaining, retaining, or accessing facial recognition
46 technology solely for the purpose of using automated or
47 semiautomated redaction software;

48
49 5. Complying with the National Child Search Assistance Act, 34
50 U.S.C. §§ 41307-413087, or other federal statutes requiring
51 cooperation in the search for missing or exploited children; or

1
2 6. Participate in, coordinate with, or otherwise be involved with
3 multi-agency law enforcement investigations, working groups
4 or task forces.

5
6 B. It shall not be a violation of this chapter for the municipality to acquire,
7 obtain, or retain facial recognition technology when all the following
8 conditions exist:

9
10 1. The facial recognition technology is an integrated, off the shelf
11 capability, bundled with software or stored on a product or
12 device;

13
14 2. Other functions of the software, product, or device are
15 necessary or beneficial to the performance of municipal
16 functions;

17
18 3. The software, product, or device is not acquired for the purpose
19 of performing facial recognition;

20
21 4. The facial recognition technology cannot be deleted from the
22 software, product, or device;

23
24 5. The municipality does not use the facial recognition technology;
25 and

26
27 6. The municipal department, agency or official seeking to acquire
28 the software, product, or device discloses the integrated, off the
29 shelf facial recognition technology that cannot be deleted to the
30 Assembly when seeking to acquire the software, product, or
31 device.

32
33 C. Recognizing that changes in technology and circumstances may
34 require additional exceptions to the requirements of this section, the
35 assembly may approve such additional exceptions by resolution,
36 under the following conditions:

37
38 1. Any municipal department that requests an exception to the
39 restrictions of section 3.102.020 shall include in its request to
40 the assembly an explanation of the need for an exception, a
41 description of how the technology or information will be used,
42 and a plan for monitoring the technology or information to
43 ensure that its use remains within the approved parameters.

44
45 2. The assembly may approve the proposed exception by
46 resolution, with or without revisions and conditions, for a period
47 of no longer than 90 days, if it finds that the exception is
48 consistent with the stated goals of preventing discrimination
49 and promoting privacy, transparency, and the public trust.

50
51 3. Upon conclusion of the period of temporary exception, the

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

- 5
6 4. A department that has obtained a permanent exception shall
7 submit an annual summary of its uses of the technology or
8 information as part of the Annual Surveillance Report under
9 Section 3.102.040 to the assembly. This summary shall not
10 include personally identifiable information.

11
12 D. Additional permanent exceptions.

- 13
14 1. Reserved.

15
16 **3.102.040. - Reports of municipal use of surveillance technologies**
17 **required.**

- 18
19 A. No later than June 1 of each year, the mayor or a designee shall
20 transmit to the assembly and cause to be publicly posted on the
21 municipal website an Annual Surveillance Report with all the following
22 information:

- 23
24 1. For each municipal department and agency that used a UAS in
25 the preceding calendar year:

- 26
27 a. The number of instances in which a UAS was used;
28
29 b. A general description of the type and purpose of each
30 instance that sufficiently explains how the use was not
31 prohibited by this chapter, and, if applicable, whether the
32 use was pursuant to a search warrant, a court order, or
33 a judicially recognized exception to the warrant
34 requirement, and the final disposition of evidence
35 resulting from each instance; and
36
37 c. Any new policy, or change in department or agency
38 policy, related to the use of UAS or Facial Recognition
39 Technology

- 40
41 2. For each municipal department or agency using Facial
42 Recognition Technology under an exception under section
43 3.102.030:

- 44
45 a. The number of instances in which Facial Recognition
46 Technology was used or information derived from Facial
47 Recognition Technology was received or used under
48 exceptions in subsections 3.102.030A.4., A.5., A.6., C.
49 and D.;
50
51 b. A general description of the type and purpose of each

1 instance that sufficiently explains how the use was not
2 prohibited by this chapter, and, if applicable, whether the
3 use was pursuant to a search warrant, a court order, or
4 a judicially recognized exception to the warrant
5 requirement, and the final disposition of evidence
6 resulting from each instance; and

7
8 c. Any new policy, or change in department or agency
9 policy, related to the use of Facial Recognition
10 Technology

11
12
13 3. The annual report shall also include the following information:

14
15 a. The number of arrests made by APD where UAS was
16 utilized in a related incident response or investigation,
17 regardless of whether the information gathered from the
18 UAS was used to establish probable cause.

19
20 b. The detailed log of every unauthorized receipt, access,
21 or use of Facial Recognition Technology or information
22 derived from Facial Recognition Technology. The log
23 shall denote how the unauthorized access occurred,
24 what corrective steps have been taken, and the final
25 disposition of any evidence or information improperly
26 received.

27
28 (AO No. 2018-5, § 1, 2-13-18)

29
30 **3.102.050. Enforcement.**

31
32 A. Any municipal employee who violates a provision of this chapter may
33 be subject to discipline in accordance with the municipality's
34 disciplinary policies and procedures and applicable collective
35 bargaining agreements. Violation of this ordinance by any official or
36 employee of the municipal is grounds for suspension or termination.
37 The disciplinary action may require the violator to participate in
38 retraining.

39
40 B. Private cause of action.

41
42 1. Any violation of this article constitutes an injury and any person
43 so injured may institute proceedings in the Superior Court in a
44 civil action seeking injunctive relief, declaratory relief,
45 damages, and attorney's fees. Any action instituted under this
46 paragraph shall be brought against the municipality. If
47 applicable, such action may also be brought against any third
48 party with whom the municipality contracted or entered into an
49 agreement.

50
51 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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32