ORDINANCE

By Fletcher

Amending Title 2, Chapter 41 of the Minneapolis Code of Ordinances relating to Administration: Information Governance.

The City Council of the City of Minneapolis do ordain as follows:

Section 1. That Chapter 41 of the Minneapolis Code of Ordinances be amended by reorganizing Sections 41.10 through 41.30 into Article I, In General, to read as follows:

ARTICLE I. – IN GENERAL

41.10. - Authorization and purpose. (a) *Purpose.* This chapter establishes an information governance program that complies with applicable laws and regulations relating to the retention, access, and disposition of city records, including the Official Records Act, Minnesota Statutes § 15.17, the Minnesota Records Management Law, Minnesota Statutes § 138.17, and the Data Practices Act, Minnesota Statutes Chapter 13.

(b) *Definitions.* Words and phrases in this chapter have the same meaning they have in the Minnesota Records Management Law, Minnesota Statutes § 138.17, and the Data Practices Act, Minnesota Statutes Chapter 13.

41.20. - Information governance program. (a) *Scope.* The information governance program applies to all city departments, personnel, and officials. All city records and data will be managed in accordance with this program.

(b) *Program.* The information governance program shall:

(1) Establish standards for managing city records and data, including electronic data, from creation through final disposition, including managing creation, access, use, security, storage, retention, and disposition.

(2) Standardize information governance practices among city departments, to the extent practicable.

(3) Establish training requirements for all staff, including specialized training for roles identified in section 41.30.

(4) Promote the maintenance of records and data in a format that facilitates sharing public data.

41.30. - Roles and Responsibilities. (a) *Information governance policy committee.* An information governance policy committee shall be responsible for policy development to govern the maintenance and implementation of the information governance program. The committee shall be comprised of the city clerk, the city coordinator, the chief information officer, and the city attorney. The committee shall meet at least quarterly. The committee shall:

(1) Review and revise existing city policies and direct development of and adopt new policies as appropriate to implement and maintain the information governance program.

(2) Report at least annually to city council on the implementation of the information governance program.

(b) *Department heads.* Department heads are responsible for the information assets created, maintained, and used by their department and for ensuring their department is in compliance with the information governance program. Each department head shall appoint a senior-level executive as the department records and data liaison and notify the city clerk of the appointment.

(c) *Departmental records and data liaisons.* Within each department, a senior official shall be responsible for implementing the information governance program. The department records and data liaison shall:

(1) Implement and maintain the information governance program in that department.

(2) Assign appropriate department and division personnel to implement and maintain the information governance program.

(3) Promulgate departmental procedures and training that effectively implement and are consistent with the city's information governance program.

(4) Ensure that the department's records and data are maintained in accordance with the information governance program.

Section 2. That Chapter 41 of the Minneapolis Code of Ordinances be amended by adding thereto a new Article II, Facial Recognition Technology, including Sections 41.100 through 41.180, to read as follows:

CHAPTER 41, ARTICLE II. – FACIAL RECOGNITION TECHNOLOGY

41.100. – Findings; Purpose. The City Council makes the following findings:

(a) As a home rule charter city, Minneapolis has broad authority through its police powers to adopt regulations to further the public health, safety, and general welfare.

(b) Discrimination in all of its forms adversely affects and degrades the health, welfare, and safety of the City. Technology that creates or perpetuates discrimination is harmful to the community.

(c) Facial recognition technology has been shown to be less accurate in identifying people of color and women. Facial recognition technology has the potential to further harm already disadvantaged communities through incorrect identifications.

(d) Facial recognition technology also has the potential to be used to increase surveillance of communities of color. This would further disproportionately harm communities that historically have faced elevated levels of policing and harassment.

(e) The City values the privacy of individuals and has adopted Data Privacy Principles. These principles include collecting information on individuals only when there is a reason to do so and being transparent about what data is being collected and why. Facial recognition technology has the potential to undermine

and conflict with these City values by increasing the amount of data collected about individuals and the likelihood that data will be collected without transparency.

(f) Facial recognition technology raises unique concerns about intrusiveness, transparency, and public trust in government. The City's use of facial recognition technology to surveil public places would be uniquely intrusive to all who live in, work in, or visit the City, and would harm the public trust in City government.

(g) The City values, respects, and protects the First Amendment right to freedom of speech. Use of facial recognition technology to surveil public places has the potential to chill the exercise of free speech in those public places.

(h) For all of the foregoing reasons, the City desires to prevent discrimination and promote privacy, transparency, and public trust by adopting a ban on City acquisition of facial recognition technology.

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

City means the City of Minneapolis and any City department, board, commission, officer or employee acting on behalf of the City.

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 the individual's face.

Facial Recognition Technology means any computer software or application that performs facial recognition.

41.120. – City Not to Acquire or Use Facial Recognition Technology. (a) Unless expressly permitted by this Article, it shall be unlawful for the City to:

(1) Acquire, obtain, or retain facial recognition technology;

(2) Enter into a contract with a third party for the purpose of acquiring, obtaining, or retaining City access to facial recognition technology; or

(3) Enter into a contract with a third party that assists the third party in developing, improving, or expanding the capabilities of facial recognition technology or provides the third party with access to information that assists the third party in doing so.

(b) Unless expressly permitted by this Article, it shall be unlawful for the City to intentionally or knowingly request, acquire, or use information obtained from facial recognition technology. The City's inadvertent or unintentional acquisition or use of information obtained from facial recognition technology shall not violate this subsection. However, upon discovery of the inadvertent or unintentional acquisition or use of information obtained from facial recognition technology, the information shall not be further used and shall be deleted to the extent permitted by law.

41.130. – Exceptions. (a) Nothing in this Article shall prevent the City from:

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

(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 City does not intentionally use the facial recognition technology;

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

(4) Having custody or control of electronic devices that include facial recognition technology when such electronic devices are held by the City solely for evidentiary purposes;

(5) Acquiring, obtaining, retaining, or accessing facial recognition technology, or using information obtained from facial recognition technology, solely for the purpose of controlling City employee access to or providing security for City workplaces that are not open to the public, provided that employees shall be permitted to opt out of using such technology to access the workplace;

(6) 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.

(b) It shall not be a violation of this Article for the City to acquire, obtain, or retain facial recognition technology under the following conditions:

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

(2) Other functions of the software, product, or device are necessary or beneficial to the performance of City functions, and

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

(4) The facial recognition technology cannot be deleted from the software, product, or device, and

(5) The City does not use the facial recognition technology, and

(6) The City department seeking to acquire the software, product, or device discloses the integrated, off the shelf facial recognition technology that cannot be deleted to the City Council 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 Article, the City Council may permit additional exceptions to the requirements of this Article, under the following conditions:

(1) Any City department that requests an exception to the requirements of this Article shall include in its request to the Council 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 Council shall hold a public hearing on any proposed exception to the requirements of this Article.

(3) The Council may approve the proposed exception if it finds that the exception is consistent with the stated goals of preventing discrimination and promoting privacy, transparency, and public trust. The Council may require revisions to the proposed plan for monitoring the technology or information as a condition of approval.

(4) The department that has obtained the exception shall annually submit a summary of its uses of the technology or information to the City Clerk. This summary shall not include personally identifiable information or information that is not public pursuant to Minnesota Statutes Chap. 13. The summary shall be included in the annual report required by Section 41.180.

41.140. – Enforcement. (a) No data or information obtained through a violation of this Article shall be received as evidence in any legislative, administrative, regulatory, or other proceeding under the City's jurisdiction.

(b) Upon the discovery of a violation of this Article, the affected Department, Board or Commission shall:

(1) Delete any data or information obtained through the violation of this Article, to the extent permitted by law.

(2) Provide a summary of the nature of the violation and steps taken to delete the data to the City Clerk for inclusion in the report described in Section 41.180.

(c) Any City officer or employee who intentionally violates this Article shall be subject to discipline, consistent with any applicable collective bargaining agreement and other applicable law, policies and procedures.

(d) Nothing in this Article shall be construed to limit any person's rights or remedies under any Federal or State law.

41.150. – Preemption. Nothing in this Article shall be interpreted or applied so as to create any power or duty in conflict with federal or state law.

41.160. – No assumption of liability. In undertaking the adoption and enforcement of this Article, the City is undertaking only to preserve and protect safety, health, and general welfare. The City is not assuming liability, nor is it imposing on its officers and employees an obligation for breach of which it is liable in money damages to any person who claims that such breach proximately caused injury. This section shall not be interpreted to preclude a petition for writ of mandamus seeking to compel the City's compliance with this Article.

41.170. – Severability. If any of parts or provisions of this Article or the application thereof to any circumstance is held invalid by a court of competent jurisdiction, the reminder of this Article, including the application of such part or provision to circumstances other than those to which is has been held invalid, shall not be affected and shall continue in full force and effect. To this end, the provisions of this Article are severable.

41.180. – Reporting. Beginning one (1) year after the effective date and annually thereafter, the City Clerk shall provide a written report to the appropriate committee of the City Council regarding the City's compliance with this Article. This report shall include a summary of any identified violations and any action taken to remedy the violation, but shall not identify any person involved or include personally identifiable information or information that is not public pursuant to Minnesota Statutes Chapter 13.