01

ORDINANCE NO. 7,676-N.S.

AMENDING BERKELEY MUNICIPAL CODE CHAPTER 2.99 TO PROHIBIT CITY USE OF FACE RECOGNITION TECHNOLOGY

BE IT ORDAINED by the Council of the City of Berkeley as follows:

Section 1. That the Berkeley Municipal Code Section 2.99.020 is amended to read as follows:

2.99.020 Definitions

The following definitions apply to this Chapter:

1. "Surveillance Technology" means an electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group. Examples of covered Surveillance Technology include, but are not limited to: cell site simulators (Stingrays); automatic license plate readers; body worn cameras; gunshot detectors (ShotSpotter); facial recognition software; thermal imaging systems, except as allowed under Section 1(d); social media analytics software; gait analysis software; and video cameras that record audio or video and can remotely transmit or can be remotely accessed.

"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 in Section 1 (above):

a. Routine office hardware, such as televisions, computers and printers, that is in widespread public use and will not be used for any surveillance functions;

b. Handheld Parking Citation Devices, that do not automatically read license plates;

c. Manually-operated, portable digital cameras, audio recorders, and video recorders that are not to be used remotely and whose functionality is limited to manually capturing, viewing, editing and downloading video and/or audio recordings, but not including body worn cameras;

d. Devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles or thermal imaging cameras used for fire operations, search and rescue operations and missing person searches, and equipment used in active searches for wanted suspects;

e. Manually-operated technological devices that are not designed and will not be used to surreptitiously collect surveillance data, such as two-way radios, email systems

and city-issued cell phones;

f. Municipal agency databases;

g. Medical equipment used to diagnose, treat, or prevent disease or injury, including electrocardiogram machines;

h. Cybersecurity capabilities, technologies and systems used by the City of Berkeley Department of Information Technology to predict, monitor for, prevent, and protect technology infrastructure and systems owned and operated by the City of Berkeley from potential cybersecurity events and cyber-forensic based investigations and prosecutions of illegal computer based activity;

i. Stationary security cameras affixed to City property or facilities.

j. Personal communication device, which means a cellular telephone, a personal digital assistant, a wireless capable tablet or similar wireless two-way communications and/or portable Internet accessing device, that has not been modified beyond stock manufacturer capabilities, whether procured or subsidized by a City entity or personally owned, that is used in the regular course of conducting City business.

2. "Surveillance Technology Report" means an annual written report by the City Manager covering all of the City of Berkeley's Surveillance Technologies that includes all of the following information with regard to each type of Surveillance Technology:

a. Description: A description of all non-privileged and non-confidential information about use of the Surveillance Technology, including but not limited to the quantity of data gathered and sharing of data, if any, with outside entities. If sharing has occurred, the report shall include general, non-privileged and non-confidential information about recipient entities, including the names of the entities and purposes for such sharing;

b. Geographic Deployment: Where applicable, non-privileged and non-confidential information about where the surveillance technology was deployed geographically;

c. Complaints: A summary of each complaint, if any, received by the City about the Surveillance Technology;

d. Audits and Violations: The results of any non-privileged internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response;

e. Data Breaches: Non-privileged and non-confidential information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response;

f. Effectiveness: Information that helps the community assess whether the Surveillance Technology has been effective in achieving its identified outcomes;

g. Costs: Total annual costs for the Surveillance Technology, including personnel and other ongoing costs.

3. "Surveillance Acquisition Report" means a publicly-released written report produced prior to acquisition or to proposed permanent use after use in Exigent Circumstances pursuant to Section 2.99.040 (2), of a type of Surveillance Technology that includes the following:

a. Description: Information describing the Surveillance Technology and how it works, including product descriptions from manufacturers;

b. Purpose: Information on the proposed purpose(s) for the Surveillance Technology;

c. Location: The general location(s) it may be deployed and reasons for deployment;

d. Impact: An assessment identifying potential impacts on civil liberties and civil rights including but not limited to potential disparate or adverse impacts on any communities or groups;

e. Mitigation: Information regarding technical and procedural measures that can be implemented to appropriately safeguard the public from any impacts identified in subsection (d);

f. Data Types and Sources: A list of the sources of data proposed to be collected, analyzed, or processed by the Surveillance Technology, including "open source" data;

g. Data Security: Information about the steps that can be taken to ensure adequate security measures to safeguard the data collected or generated from unauthorized access or disclosure;

h. Fiscal Cost: The fiscal costs for the Surveillance Technology, including initial purchase, personnel and other ongoing costs, including to the extent practicable costs associated with compliance with this and other reporting and oversight requirements, as well as any current or potential sources of funding;

i. Third Party Dependence and Access: Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis, and whether a third party may have access to such data or may have the right to sell or otherwise share the data in aggregated, disaggregated, raw or any other formats;

j. Alternatives: A summary and general assessment of potentially viable alternative methods (whether involving the use of a new technology or not), if any, considered before

deciding to propose acquiring the Surveillance Technology; and

k. Experience of Other Entities: To the extent such information is available, a summary of the experience of comparable government entities with the proposed technology, including any unanticipated financial or community costs and benefits, experienced by such other entities.

4. "Surveillance Use Policy" means a publicly-released and legally-enforceable policy for use of each type of the Surveillance Technology that shall reflect the Surveillance Acquisition Report produced for that Surveillance Technology and that at a minimum specifies the following:

a. Purpose: The specific purpose(s) that the Surveillance Technology is intended to advance;

b. Authorized Use: The uses that are authorized, the rules and processes required prior to such use, and the uses that are prohibited;

c. Data Collection: Information collection that is allowed and prohibited. Where applicable, list any data sources the technology will rely upon, including "open source" data;

d. Data Access: A general description of the title and position of the employees and entities authorized to access or use the collected information, and the rules and processes required prior to access or use of the information, and a description of any and all of the vendor’s rights to access and use, sell or otherwise share information for any purpose;

e. Data Protection: A general description of the safeguards that protect information from unauthorized access, including encryption and access control mechanisms, and safeguards that exist to protect data at the vendor level;

f. Civil Liberties and Rights Protection: A general description of the safeguards that protect against the use of the Surveillance Technology and any data resulting from its use in a way that violates or infringes on civil rights and liberties, including but not limited to potential disparate or adverse impacts on any communities or groups;

g. Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond such period;

h. Public Access: How collected information may be accessed or used by members of the public;

i. Third Party Data Sharing: If and how other City or non-City Entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information;

j. Training: Training required for any employee authorized to use the Surveillance Technology or to access information collected;

k. Auditing and Oversight: Mechanisms to ensure that the Surveillance Use Policy is followed, technical measures to monitor for misuse, and the legally enforceable sanctions for intentional violations of the policy; and

l. Maintenance: The mechanisms and procedures to ensure maintenance of the security and integrity of the Surveillance Technology and collected information.

5. "Exigent Circumstances" means the City Manager's good faith belief that an emergency involving imminent danger of death or serious physical injury to any person, or imminent danger of significant property damage, requires use of the Surveillance Technology or the information it provides.

6. "Face Recognition Technology" means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face.

Section 2. That the Berkeley Municipal Code Section 2.99.030 is amended to read as follows:

2.99.030 City Council Approval Requirement

1. The City Manager must obtain City Council approval, except in Exigent Circumstances, by placing an item on the Action Calendar at a duly noticed meeting of the City Council prior to any of the following:

a. Seeking, soliciting, or accepting grant funds for the purchase of, or in-kind or other donations of, Surveillance Technology;

b. Acquiring new Surveillance Technology, including but not limited to procuring such technology without the exchange of monies or consideration;

c. Using new Surveillance Technology, or using Surveillance Technology previously approved by the City Council for a purpose, or in a manner not previously approved by the City Council; or

d. Entering into an agreement with a non-City entity to acquire, share or otherwise use Surveillance Technology or the information it provides, or expanding a vendor's permission to share or otherwise use Surveillance Technology or the information it provides.

2. The City Manager must present a Surveillance Use Policy for each Surveillance Technology to the Police Review Commission, prior to adoption by the City Council. The Police Review Commission shall also be provided with the corresponding Surveillance Acquisition Report that had been presented to council for that Surveillance Technology. No later than 30 days after receiving a Surveillance Use Policy for review, the Police Review Commission must vote to recommend approval of the policy, object to the proposal, recommend modifications, or take no action. Neither opposition to approval of such a policy, nor failure by the Police Review Commission to act, shall prohibit the City Manager from proceeding with its own review and potential adoption.

3. The City Manager must submit for review a Surveillance Acquisition Report and obtain City Council approval of a Surveillance Use Policy prior to engaging in any of the activities described in subsections (1) (a)-(d).

4. Evidence received relating to the investigation of a specific crime that may have been generated from Face Recognition Technology but was not intentionally solicited shall not be a violation of this ordinance.

5. Notwithstanding any other provision of this Chapter, it shall be a violation of this ordinance for the City Manager or any person acting on the City Manager's behalf to obtain, retain, request, access, or use: i) any Face Recognition Technology; or ii) any information obtained from Face Recognition Technology, except for personal communication devices as defined by Section 2.99.020 or section 2.99.030(4). The inadvertent or unintentional receipt, access to, or use of any information obtained from Face Recognition Technology shall not be a violation of this subsection provided that the City Manager or any person acting on the City Manager's behalf does not request or solicit the receipt, access to, or use of such information, and all copies of the information are promptly destroyed upon discovery of the information, and the information is not used for any purpose.

The City Manager shall log the receipt, access to, or use of any such information in its Annual Surveillance Technology Report. The Surveillance Technology Report shall identify measures taken by the City to prevent the further transmission or use of any information inadvertently or unintentionally obtained through the use of Face Recognition Technology; provided, however, that nothing in this Chapter shall limit the ability to use such information in connection with a criminal investigation.

Section 3. Copies of this Ordinance shall be posted for two days prior to adoption in the display case located near the walkway in front of the Maudelle Shirek Building, 2134 Martin Luther King Jr. Way. Within 15 days of adoption, copies of this Ordinance shall be filed at each branch of the Berkeley Public Library and the title shall be published in a newspaper of general circulation.

At a regular meeting of the Council of the City of Berkeley held on October 15, 2019, this Ordinance was passed to print and ordered published by posting by the following vote:

Ayes: Bartlett, Davila, Droste, Hahn, Harrison, Kesarwani, Robinson, Wengraf, and Arreguin.

Noes: None.

Absent: None.