CITY OF MADISON, WISCONSIN

AN ORDINANCE

Creating Section 23.61 of the Madison General Ordinances to establish Surveillance Technology guidelines for Departments.

PRESENTED
REFERRED President's Work Group to Develop City-Wide Surveillance Equipment & Data Management Policies

Drafted by: Marci Paulsen

Date: March 11, 2019

SPONSORS: Alder Kemble, Alder Baldeh, Alder Carter

DRAFTER'S ANALYSIS: This ordinance establishes several definitions including surveillance data and surveillance technology. The ordinance requires all Departments to obtain approval from the Mayor and Common Council before obtaining or using surveillance technology. It requires all Departments to provide public notice and to hold a public meeting whenever the Department plans to obtain or use new surveillance technology. The ordinance requires all Departments to provide an annual report on its use of surveillance technology to the Common Council and public. The ordinance creates several exceptions for the approval process outlined within the ordinance, including when there is an emergency situation or when the surveillance technology involves information that must remain confidential. The ordinance establishes an oversight board to review the exception of sensitive surveillance technology.

****

The Common Council of the City of Madison do hereby ordain as follows:

1. Section 23.61 entitled "Use of Surveillance Technology" of the Madison General Ordinances is created to read as follows:

"**23.61 USE OF SURVEILLANCE TECHNOLOGY.**

(1) Intent and Purpose. City of Madison agencies have identified a wide variety of legitimate business reasons to use surveillance technology. The Common Council recognizes the need to carefully balance the need for surveillance for public safety and prosecution of crimes with the public's right to privacy and protection from unreasonable searches and protection of civil liberties including freedom of speech or association. The Common Council desires to adopt a city-wide surveillance technology and surveillance data management policy that is consistent for all City Departments and covers all type of surveillance equipment usage and surveillance data management.

(2) Definitions.

"Chief Information Officer" means the head of the City Information Technology Department.

"Department" means any agency, department, or division of the City.

"Surveillance" means observation of a place, person, group, or ongoing activity in order to gather information.

"Sensitive Surveillance Technology Oversight Board (SSTOB)" means a board which reviews exceptions to this section. The SSTOB members are the Mayor, the Common Council President, and the Chief Information Officer.

"Surveillance data" means any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by surveillance technology.

Approved as to form:

"Surveillance technology" means any hardware, software, electronic device, or system utilizing an electronic device, owned by the City or under contract with the City, designed, or primarily intended, to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory or other personally identifiable information of members of the public for the purpose of surveillance. Surveillance technology includes but is not limited to the following: cell site simulators; automatic license plate readers; gunshot detection systems; facial recognition software; gait analysis software; video cameras that record audio or video and can transmit or be remotely accessed; and unmanned aircraft systems equipped with remote video capabilities. Surveillance technology does not include the following devices:

1. Office hardware, such as televisions, computers, credit card machines, copy machines, telephones and printers, that are widespread in use by the City;
2. Audio/video teleconference systems;
3. City databases and enterprise systems that contain information, including, but not limited to, human resource, permit, license and business records;
4. City databases and enterprise systems that do not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology, including payroll, accounting, or other fiscal databases;
5. Information technology security systems, including firewalls and other cybersecurity systems;
6. Systems or databases that capture information where an individual knowingly and voluntarily consented to provide the information, such as applying for a permit, license or reporting an issue;
7. Physical access control systems, employee identification management systems, and other physical control systems;
8. Infrastructure and mechanical control systems, including those that control or manage street lights, traffic lights, or water or sewer functions;
9. Manually-operated technological devices used primarily for internal City and Department communications and are not designed to surreptitiously collect surveillance data, such as radios, cell phones, personal communications devices and email systems;
10. Manually-operated, non-wearable, handheld cameras, audio recorders and video recorders that are not designated to be used surreptitiously and whose function is limited to manually capturing and manually downloading video and/or audio recordings;
11. Devices that cannot record or transmit audio or video or electronic data or be remotely accessed, such as vision-stabilizing binoculars or night vision goggles;
12. Computers, software, hardware or devices used in monitoring the work and work-related activities involving City buildings, employees, contractors and volunteers or used in conducting internal investigations involving City employees, contractors and volunteers;
13. Medical equipment and systems used to record, diagnose, treat, or prevent disease or injury and are used and/or kept in the course of providing City services;
14. Parking Ticket Devices;
15. Equipment used on a temporary basis for investigations and in accordance with City policies;
16. Cameras intended to record activities at City facilities in nonpublic areas;
17. Police Department interview rooms, holding cells, and Police Department internal security audio/video recording systems; and
18. Police Department records/case management systems, Live Scan, Computer Aided Dispatch (CAD).

(3) Surveillance Review Team

a. A Surveillance Review Team ("SRT") is hereby created to establish overall enterprise policy, insure consistency among Departments and to review the potential impact of Surveillance Technology on civil liberties or privacy and approve any proposed changes to the Administrative Procedures Memorandum (APM) related to surveillance technology. The SRT

will consist of the Common Council Chief of Staff and a designee from each of the following departments: Mayor's Office, Police, Information Technology, City Attorney, Finance, Civil Rights, Metro, Water Utility, and Traffic Engineering.

(4) Applicability. This ordinance applies to all Departments that do any of the following:

(a) Seek funds for new surveillance technology including applying or accepting grants, state or federal funds or other donations;

(b) Acquire new surveillance technology, with or without a cost;

(c) Use surveillance technology for a purpose or in a manner or in a location not previously approved; or

(d) Enters into an agreement with any other entity to share surveillance technology or surveillance data.

(5) Approval Process. The SRT will establish an approval process for use of surveillance technology and equipment no later than October 31st 2019. As of January 1st 2020, all Departments must comply with this subsection prior to any use of surveillance technology.

(a) Departments shall submit a request in writing to the Common Council for the purchase and/or use of surveillance technology per subsection (3). The request shall be in the form of a report and shall include the information specified in the APM related to the approval process for surveillance technology, as applicable.

(b) The Department will post notice of its intent to obtain or use surveillance technology to the public on the City of Madison website and will notify all alders. The Department will hold a public engagement meeting per the process established by the SRT. The Department may amend the initial request based on public comment and submit the amended request to the Common Council.

(c) The Department's request for surveillance technology will be approved by the Common Council only upon the determination that the benefits to the citizens and residents of the City outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the judgment of the Common Council, no alternative with a lesser economic cost or impact upon civil rights or civil liberties would be as effective.

(6) Annual Report.

(a) Each Department will conduct an annual review of its surveillance technology and insure compliance with this section. Each Department will complete an Annual Surveillance Technology Report. (b) The Annual Surveillance Technology Report will include:

1. An inventory of current surveillance technology and the applicable policies;
2. How the Department has used the data collected by its surveillance technology;
3. How any surveillance data is being shared with other entities;
4. How well surveillance data management protocols are safeguarding individual information;
5 Whether the Department has received any complaints or concerns about its surveillance technology use.

(c) The SRT shall audit the Annual Surveillance Technology Reports for accuracy and completeness. The Chief Information Officer will provide a report containing the results of the audits, along with the departmental reports, annually to the Common Council through resolution.

(d) The Common Council shall review and take action on the Annual Surveillance Technology Reports and the Chief Information Officer's audit. Approval for the use of surveillance technology may be rescinded by the Common Council or modified by the Common Council through resolution.

(7) Noncompliance. The Mayor shall direct any Department out of compliance with this section to remedy the deficiency and report back in a timely manner how the Department has gained compliance. Surveillance technology may not be used to visually or audibly monitor the interior of private dwellings where a reasonable expectation of privacy exists, absent a court order or other lawful justification. Any violation of this ordinance by staff shall be subject to City disciplinary processes.

(8) Exceptions.

(a) Federal Property Disposition Programs. If the surveillance technology is available through federal property disposition programs and the purchase or acquisition

decision must be executed quickly, such acquisition may be made. However, if the surveillance technology is obtained under this subdivision, the Department must apply for approval as described in subsection (4) before installation or use of said equipment. If approval is denied the surveillance technology shall be returned within sixty (60) days after approval was denied.

(b) Emergency Situations. In the event of an emergency situation that poses an imminent and serious risk of death or substantial bodily harm, a Department may acquire surveillance technology without prior Common Council approval, for the sole purpose of preventing or mitigating such risk, if the Department reasonably believes the acquisition of such surveillance technology will result in reduction of said risk. The Department's use of the surveillance technology must cease when such risk no longer exists or the use of the surveillance technology can no longer reasonably reduce the risk. The department shall apply for approval of the surveillance technology per subsection 5 of this ordinance within fourteen (14) days of cessation of the risk that prompted purchase of said technology. The use of the surveillance technology must be documented in the Department's Annual Surveillance Technology Report.

(c) Technical Patch or Upgrade. A Department, in consultation with the City IT Department without approval, may apply a technical patch or upgrade that is necessary to mitigate threats to the City's infrastructure, even if the patch or upgrade materially alters the surveillance capabilities of the technology. However, such patch or upgrade, if it does materially alter the surveillance capability of the technology, must be highlighted in the Annual Surveillance Technology Report.

(d) Sensitive Information and Data. Departments that use surveillance technology that is of a sensitive or confidential nature may utilize an alternative approval process to use said technology through the Sensitive Surveillance Technology Oversight Board (SSTOB). Departments shall submit an explanation of why the surveillance technology is considered sensitive, along with all required elements of this section to the SSTOB for review and approval. The SSTOB shall evaluate the proposal and make a determination regarding approval within thirty (30) days of a complete application. The SSTOB may revoke approval for a surveillance technology at any time, at which time it may no longer be used. The Chief Information Officer shall maintain the records of all sensitive technology reviewed by the SSTOB.