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 / President's Work Group

Date: March 11, 2019

SPONSORS: Alder Kemble

DRAFT

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.

"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.

Commented [KK1]: Changed by workgroup

Commented [KK2]: Changed by workgroup

Approved as to form:

Michael P. May, City Attorney

"Surveillance technology" means any 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 t ~~T~~echnology does not include the following devices, hardware or software:

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 court of providing City services;
14. Parking Ticket Devices;
15. Equipment used on a temporary basis for investigations and in accordance with City policies;
~~15.~~16. Cameras intended to record activities at City facilities in nonpublic areas;
~~16.~~17. Police Department interview rooms, holding cells, and police Department internal security audio/video recording systems; and
~~17.~~18. Police Department ~~systems and databases, including but not limited to,~~ records/case management systems, Live Scan, Computer Aided Dispatch (CAD).

(3) 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;

Commented [KK3]: Change requested by Alders Kemble & Zellers

Commented [KK4]: Changed by workgroup

Commented [KK5]: Added by workgroup

Commented [KK6]: Changed by workgroup

(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.

(4) Approval Process. Prior to any use of surveillance technology all Departments must comply with this subsection.

(a) Departments shall submit a request in writing ~~for~~ to the Common Council for the purchase and/or use of surveillance technology per MGO 23.61(3). The request ~~should~~ shall be in the form of a report and ~~should~~ shall include the following, as applicable:

1 A description of the surveillance technology, its capabilities and the surveillance data or information it will generate.

2. A surveillance technology use policy ~~including~~, which will include the following:

a. ~~Who is t~~The lead Department responsible for the surveillance technology;

b. The training protocols the Department will put in place, which shall minimally include appropriate uses of surveillance technology and access to data;;

c. The intended location and/or deployment of the surveillance technology;

d. How and when the Department will use the surveillance technology;

e. How the surveillance technology will be captured, including whether it will be by real-time or historical data capture;

f. Whether there are any privacy rights affected by the surveillance technology. If there is the potential for a privacy impact what is the Department's mitigation plan for said impact;

g. Identification of groups of people on whom this surveillance technology may have a disparate impact, and explanation of the Department's public notification plan for each potentially disparately impacted group; ~~Whether the surveillance technology potentially has an impact on any minority groups. What is the Department's public notification plan for each group potentially impacted~~;

h. ~~What is t~~The potential fiscal impact of the surveillance technology;

i. Whether the Department has agreements with other entities for the use or access of the surveillance technology;

j. How the surveillance technology access and usage will be shared, managed and monitored;

k. Who will be using the surveillance technology;

l. How the surveillance technology will be used; and

m. How the surveillance date will be stored, retained and deleted.

(b) The Department will post ~~notice of~~ notice of its ~~plan~~ intent to obtain or use surveillance technology to the public on the website dedicated for that purpose, and will notify all alders. The Department will hold a public engagement meeting at least thirty (30) days after posting the notice. The public engagement meeting will be accessible, be noticed in multiple languages, and be held in communities potentially impacted by the proposed use or acquisition of the surveillance technology. The Department will collect information about potential disparate impacts. ~~on disadvantaged groups.~~ 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 ~~accepted~~ 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.

(54) Annual ~~Review~~Report.

(a) Each Department will conduct an annual ~~audit~~ review of its surveillance technology and insure compliance with this section. Each Department will complete an Annual

Commented [KK7]: Changed by workkgroup

Commented [KK8]: Change requested by Alders Kemble & Zellers

Commented [KK9]: Changed by workgroup

Commented [KK10]: Change requested by Alder Kemble and Zellers

Commented [KK11]: Changed by workgroup

Commented [PM12]: How are they going to be able to do this? From who?

Commented [KK13]: Changed by workgroup

Commented [KK14]: Change requested by Alders Kemble & Zellers

Commented [KK15]: Changed by workgroup

Surveillance Technology Report.t ~~that will be audited by the Chief Information Officer and provided to the Common Council and the public. Who will have an opportunity to comment on the 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 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. ~~How the surveillance technology has impacted or could impact civil liberties on disadvantaged populations;~~
6. ~~5.~~ Whether the Department has received any complaints or concerns about its surveillance technology use;
7. ~~6.7.~~ ~~The results of the Department's internal audit; and~~
8. ~~Whether the Department is in compliance with this section.~~

(c) The Chief Information Officer shall audit the Annual Surveillance Technology Reports for accuracy and completeness and provide the results of the audit along with the departmental reports to the Common Council.

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

(6~~5~~) Noncompliance. The Chief Information Officer ~~will~~ 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. Under no circumstances shall surveillance technology be used to visually or auditorily access private spaces. ~~Any violation of this ordinance by staff shall be subject to disciplinary processes as set forth in the Employee Handbook. Any violation of the section or the Mayor's Administrative Procedure Memorandum governing use of surveillance technology shall be handled through disciplinary processes as set forth in the Employee Handbook.~~

(7~~6~~) Exceptions.

(a) ~~Law Enforcement~~Federal Property Disposition Programs. ~~Law enforcement is exempted from this section I~~if the surveillance technology is available through federal property disposition programs and the purchase or acquisition decision must be executed quickly, such purchase may be made. However, if. ~~If~~ the surveillance technology is obtained under this subdivision, the Department must apply for approval as described in sub. (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 use of the surveillance technology must be documented in the Department's Aannual Ssurveillance ~~usage~~ Technology Rreport, and any future acquisition or use of such surveillance technology must be approved as outlined in this section prior to said use.

(c) Technical Patch or Upgrade. The City IT DepartmentA ~~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.

Commented [KK16]: Changed by workgroup

Commented [KK17]: Change requested by Alders Kemble & Zellers

Commented [PM18]: How would a department prove this?

Commented [PM19]: I removed this because I don't believe any department is going to say "we aren't in compliance with the ordinance?"

Formatted: Indent: Left: 1"

Commented [KK20]: Changed by workgroup

Formatted: Strikethrough

Commented [KK21]: Changed by workgroup

Commented [PM22]: All of this would have to come through a resolution:

Issue recommendations as necessary to improve surveillance technology usage. This may include a directive to the Department that the use of the surveillance technology cease, that modifications be made to the Department's surveillance technology use policy or that the Department provide a response to the Common Council on outlined concerns.

Commented [KK23]: Change requested by Alders Kemble & Zellers

Formatted: Indent: Left: 0.5", Hanging: 1"

Commented [KK24]: Change requested by Alders Kemble & Zellers

Commented [KK25]: Change requested by Alders Kemble & Zellers

Commented [PM26]: How is a "department" to be disciplined?

Commented [PM27]: Is this just for law enforcement or can other departments use this exception?

Commented [PM28]: Is it possible to "return" some of the technology?

Commented [KK29]: Change requested by Alders Kemble & Zellers

Commented [PM30]: Would a department do this or should it say IT?

Commented [KK31]: Changed by workgroup

(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 ~~will~~ 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 ~~will~~ shall evaluate the proposal and make a determination regarding approval within thirty (30) days of a complete application. The SSTOB ~~can~~ may revoke approval for a surveillance technology at any time, at which time it may no longer be used. The Chief Information Officer ~~will~~ shall maintain the records of all sensitive technology reviewed by the SSTOB."

Commented [PM32]: What happens if it is revoked?

Commented [KK33]: Change requested by Alders Kemble & Zellers