

1) Purpose

- I. the City of Madison has an interest in a city-wide surveillance technology and data management policy that is consistent for all City agencies and covers all type of surveillance equipment usage and data management (City of Madison Resolution 49217)
- II. the City of Madison seeks to carefully balance the need for surveillance for public safety and prosecution of crimes with the public's right to privacy and protection from warrantless search and seizure (Nashville, Santa Clara)

2) Definitions

- I. "Surveillance technology"¹ means **any** electronic device, software program, or hosted software solution that is designed or primarily intended to be used for the purpose of surveillance. (Seattle)
- II. "Surveillance" or "surveil" means to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise **concerns** about civil liberties, freedom of speech or association, racial equity or social justice. (Seattle)
- III. "Surveillance data" shall mean **any** electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by surveillance equipment. (Seattle)
- IV. "Municipal entity" shall mean any municipal government, **agency**, department bureau, division, or unity of the City of Madison. (Seattle)

Commented [PM1]: This seems way too broad and could incorporate more than was intended but I would defer to the IT experts here...I see the different definitions listed below so I'm confused on which one is being used

Commented [PM2]: Not sure why you say raise concerns?

Commented [PM3]: Again this seems very broad but I would defer to IT

Commented [PM4]: I don't think you need this definition at all

¹ "Surveillance technology" includes any electronic surveillance device, hardware, or software that is capable of collecting, capturing, recording, retaining, processing, intercepting, analyzing, monitoring, or sharing audio, visual, digital, location, thermal, biometric, or similar information or communications specifically associated with, or capable of being associated with, any specific individual or group; or any system, device, or vehicle that is equipped with an electronic surveillance device, hardware, or software.

"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 paragraph i. 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 or surveillance-related functions; (b) Parking Ticket Devices (PTDs); (c) manually-operated, non-wearable, handheld digital cameras, audio recorders, and video recorders that are not designed to be used surreptitiously and whose functionality is limited to manually capturing and manually downloading video and/or audio recordings; (d) surveillance devices that cannot record or transmit audio or video or be remotely accessed, such as image stabilizing binoculars or night vision goggles; (e) municipal agency databases that do not and will not contain any data or other information collected, captured, recorded, retained, processed, intercepted, or analyzed by surveillance technology; (f) manually operated, and (g) technology that monitors only City employees in the performance of their City functions.

3) Council approval required

I. Whenever

- i. Seeking funds
Seeking funds for surveillance technology including applying or accepting grants, state or federal funds or in-kind or other donations
- ii. Acquiring new technology
Acquiring new surveillance technology (whether or not money changed hands)
- iii. Using surveillance technology
Using surveillance technology for a purpose, in a manner, or in a location not previously approved by the Board
- iv. Entering into an agreement with other entities (excluding/including municipal entities?) to share equipment or data

(Sommerville, Santa Clara, Nashville)

Commented [PM5]: Is this intended to preempt the purchasing MGOs?
Will there be an exemption for time sensitive needs/use?

Commented [AH6]: FROM VIC WAHL

I think this should be limited to seeking funds for new or previously unused technologies. If we have to go through an onerous council approval process anytime we need to replace an in-car video system or something else that we have been using for years, that seems wasteful. I think some of the other ordinances use similar language.

Commented [AH7]: FROM VIC WAHL

As we discussed at a prior meeting, I think there needs to be a provision for an agency to accept or purchase something if there isn't time to get prior approval (the example I used was the 10-33 program) and then seek approval after the fact. Otherwise agencies may miss out on things that are valuable to their mission and serving the public.

Commented [AH8]: FROM VIC WAHL

Again, I suggest an option for time-sensitive actions where the approval comes after acquisition.

Commented [AH9]: FROM VIC WAHL

Again, I suggest an option for time-sensitive actions where the approval comes after acquisition.

Commented [PM10]: Does this just cover City equipment? What if use other entities equipment? For every single use? This appears to be too broad & not feasible as written

Commented [AH11]: FROM VIC WAHL

This section, if it will be included, really needs clarification. Clearly we cannot be expected to seek approval prior to individual investigative uses of technology. In fact, to do so in some instances would violate state law. And the scope of this needs to be clearer. If the council is approving acquisition/purchase I wonder if that isn't sufficient (as I imagine that process will incorporate a discussion on usage). This language would also seem to require (for example) council

Commented [PM12]: Does this just mean a contract? If it is meant to mean anytime the City uses equipment this is not feasible

Commented [AH13]: FROM VIC WAHL

I think this should be limited to only apply to City agencies sharing data obtained through surveillance technology with private entities for payment. We obtain information (like surveillance video) from all

II. Approval process

i. Submit request

Department shall submit request for approval to the Mayor and the Council to initiate the approval process in writing. The request should include a

(a) Description of the technology, its capabilities and the data/info it will likely generate,

(b) A surveillance use policy including; who is the lead department responsible for technology, training protocols, intended location / deployment of surveillance, how and when the department will use surveillance, real time vs. historical data capture, privacy rights affected by the surveillance, mitigation plan for privacy impacts, impacts on people of color, low income people, public notification plan for each community impacted, fiscal impact, agreements with other entities, how will equipment access and usage be shared/managed, how will access to data be shared/managed

(c) A clear use and data management policy including: how and when the tech will be used and by whom, any additional rules governing use, how data will be stored, how data will be retained and deleted, how data will be accessed, compliance/audit protocols, data retention time frames, destruction protocols, methods for storing data including metadata, whether the technology or data will be shared, efforts to ensure compliance with policy, community engagement, impacts on civil rights and liberties, fiscal impact (Seattle)

Commented [AH14]: FROM VIC WAHL

Will this process be required of technologies in use at the time the ordinance/resolution/APM (whatever the final form is) comes into effect? That will obviously be a major undertaking (Seattle's website suggests this will be at least a 2-year process for them).

Commented [PM15]: Need to have an exception for items that must be kept confidential

Commented [AH16]: FROM VIC WAHL

What about new technology that an agency determines needs to remain confidential and only shared through that process? There should be a reference to that alternate process.

Commented [PM17]: A new policy is needed every time one of the 4 items listed above occurs? Is this feasible for staff?

Commented [PM18]: What is meant by when? That is broad

Commented [PM19]: This is too broad

Commented [PM20]: Same comments as subsection (b) above

ii. Transparency

Department shall post notice of a formal request for surveillance technology approval to the public on a city website dedicated for the purpose. No less than 30 days after the public notification can the department conduct the public engagement meeting. (Seattle)

Commented [AH21]: FROM VIC WAHL

Again, I think we need the confidential process referenced here.

Commented [PM22]: Is this timeline feasible for staff? What if confidential use/device?

iii. Conduct public engagement

The Department shall conduct one or more meeting with opportunity for public comment and written response for each approval request. The community meetings should be accessible, be noticed in multiple languages, be held in communities impacted by the proposed acquisition and collect info about potential disparate impacts on disadvantaged groups. (Seattle)

Commented [AH23]: FROM VIC WAHL

The viability of this seems somewhat dependent on the final scope of the required approvals (above). If this is required for simply purchasing a new in-car video unit or adding a traffic camera to an intersection it strikes me as very unreasonable (and unnecessary).

Commented [PM24]: What is an "approval request"?

iv. Incorporate public comment and submit request

The Department will amend the initial request based on public comment and submit the amended request to the Mayor and Council. (Seattle)

Commented [PM25]: How determine this if it's a new city wide program?

Commented [PM26]: So the department is "required" to amend based on public comment?

v. Council reviews

The approval by the Common Council for any surveillance technology request as described above shall be granted only upon the determination that the benefits to the citizens and residents of the City of Madison outweigh the costs; that the proposal will safeguard civil liberties and civil rights; and that, in the judgment of the City of Madison Common Council, no alternative with a lesser economic cost or impact upon civil rights or civil liberties would be as effective. (Nashville)

Commented [AH27]: FROM VIC WAHL

I think the review process is overly formalistic and burdensome, removing discretion from the mayor and council. I can think of potential new technologies that would certainly call for this level of review and engagement, but also think of many that wouldn't, where the council and/or mayor could settle on a more informal level of review.

Commented [PM28]: Appears to be a time intensive process that may not be feasible

4) Review Measures

I. Annual Surveillance Technology Report

- i. The Chief Technology Officer and the City Auditor (Risk Manager?) shall conduct an annual review of surveillance technology and City department compliance with the ordinance. The Annual Surveillance Technology Report will be released to the public and considered by the Council. The public will have an opportunity to comment on the Annual Report.

Commented [PM29]: The Risk manager has not agreed to conduct this review nor does he have the staff to conduct such a broad time consuming review.

- ii. The Annual Report will include:

- (a) An inventory of current surveillance technology and policies
- (b) How surveillance tech has been used, usage patterns
- (c) How surveillance data is being shared with other entities
- (d) How well data management protocols are safeguarding individual info
- (e) How surveillance tech have impacted or could impact civil liberties on disadvantaged populations
- (f) Complaints or concerns about surveillance tech (including internal audits)
- (g) Total annual costs, including personnel
- (h) Whether any departments are out of compliance with the ordinance (Seattle)

Commented [AH30]: FROM VIC WAHL

This will be a massive amount of work for all agencies to comply with. I imagine it would be most effort for IT to manage this process and prepare the report. While this process is called for in some of the other ordinances it does not seem to be in line with what we need here.

Commented [PM31]: This is a huge undertaking

Commented [PM32]: How determine use? Daily – again a massive undertaking

Commented [PM33]: How can this be judged?

Commented [PM34]: What is an “internal audit”?

Commented [PM35]: Cost of what? How is this going to be calculated? Can it even be calculated?

Commented [PM36]: What ordinance?

5) Enforcement

- I. Violations resulting from arbitrary or capricious action or conduct by the County or an officer thereof in his or her official capacity, the prevailing complainant in an action for injunctive relief may collect from the County reasonable attorney's fees
- II. Intentional misuse of County-owned surveillance technology is a misdemeanor (Santa Clara)
- III. The Council will review and the Annual Surveillance Technology Report and will issue recommendations via resolution or ordinance to improve Surveillance Technology Usage each year in response to the report.
 - (b) The Council may direct that the
 - (i) use of the tech cease
 - (ii) Require modifications to a surveillance use policy
 - (iii) Department report back regarding Council concerns (Santa Clara)

Commented [AH37]: FROM VIC WAHL

An ordinance cannot create a misdemeanor. Ultimately any misuse of these technologies is primarily an employment issue for HR (or MPD/MFD) to deal with.

One thing missing from the whole discussion is audit processes...we do a number of audits in MPD but do not have the capability (at least that I know of) to audit use of the City Enterprise cameras...that would benefit us (perhaps IT has that capability).

Commented [PM38]: Can't authorize someone to sue the City

Commented [AH39]: FROM VIC WAHL

I'm sure the City Attorney will weigh in on this, but it does not strike me as good public policy to expose the City to potential financial liability by ordinance/resolution/APM.

Commented [PM40]: No authority to create a crime

Commented [PM41]: Recommendations in an ordinance? That doesn't make sense....

- IV. The Chief Tech Officer shall direct any City department out of compliance with the ordinance to cease use of surveillance tech (Seattle)
- V. A person who is surveilled and injured by a violation of the ordinance may institute proceedings against the City (Seattle)
- VI. Departments may use existing technology as long as they comply with the Ordinance (Seattle)
- VII. The Executive shall establish a process for determining whether technology is surveillance technology (Seattle)
- VIII. The Council may at any time designate that a technology is or is not surveillance technology. (Seattle)

Commented [AH42]: FROM VIC WAHL

Probably not something we want in ordinance

Commented [PM43]: Can't create a cause of action here

Commented [PM44]: This doesn't make sense

Commented [AH45]: FROM VIC WAHL This is all dependent on the scope of the approval process described above. If that process is intended to apply to individual cases, then I think this is far beyond what anyone is contemplating (and will have a significant adverse impact on police operations). So I think that the approval section needs to be clarified and limited. Whoever the confidential process involves (mayor and council president, for example) should be the ones who make the determination...I suspect that agencies may have questions and it seems wisest that they be resolved (at least initially) through the confidential process.

Commented [PM46]: How can they change what is surveillance if it's defined in ordinance/resolution?

6) Exemptions

I. Law Enforcement Exemptions

Law enforcement and governmental exemption from ordinance if the surveillance technology is:

- (a) Used on a temporary basis for the purpose of a criminal investigation supported by reasonable suspicion,
- (b) Pursuant to a lawfully issued search warrant,
- (c) Under exigent circumstances as defined in case law (Nashville)
- (d) To facilitate investigative functions of the police department (Santa Clara)
- (e) Body worn cameras, police car cameras (Seattle)
- (f) Utilized when the Chief of Police finds, subject to approval of the Mayor, that compelling circumstances in the public interest warrant temporary use (Sommerville)

- (g) Available through the military surplus program, and purchasing/acquiring decisions must be executed quickly. If the technology is purchased under this exemption, the law enforcement department must apply for approval as described in section 3) before installing or using the equipment. If approval is denied the surveillance technology shall be returned no less than 60 days after approval was denied.

Commented [AH47]: FROM VIC WAHL

This is all dependent on the scope of the approval process described above. If that process is intended to apply to individual cases, then I think this is far beyond what anyone is contemplating (and will have a significant adverse impact on police operations). So I think that the approval section needs to be clarified and limited.

Commented [PM48]: Can't expect this to occur for every individual case

Commented [PM49]: This doesn't make sense = why only military surplus? If needed quickly how have time to go through this process?

II. Emergency Situations

- (a) In the event of an emergency situation that poses an imminent and serious risk of death or substantial bodily harm, a City department may acquire surveillance technology without prior 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 the risk. The department's use of the surveillance technology must end when such risk no longer exists or the use of the surveillance technology can no longer reasonably reduce the risk. The use must be documented in the department's annual surveillance usage report, and any future acquisition or use of such surveillance technology must be approved by the City Council as set forth in this policy. (Seattle)

Commented [PM50]: Too high of a burden

Commented [PM51]: What if needs to remain confidential?

Commented [AH52]: FROM VIC WAHL

I think it would be best if this was just excluded from the definition of surveillance technology.

Commented [PM53]: What does this have to do with surveillance?

Commented [PM54]: What is the purpose of this section? Are these cameras exempt from the above requirements?

III. Technical Patch or Upgrade

- (a) A City department may apply a technical patch or upgrade that is necessary to mitigate threats to the City's environment, even if the patch or upgrade materially alters the surveillance capabilities of the technology (Seattle)

IV. Security and Traffic Cameras

- (a) Cameras on City property solely for security purposes
- (b) Cameras installed solely to protect the physical integrity of City infrastructure
- (c) Cameras installed pursuant to state law authorization in or on any vehicle or along a public right-of way solely to record traffic violations (Seattle)

Commented [PM55]: Can't use video for traffic violations – against state statute

V. City Functions

- (a) Technology that monitors only City employees in the performance of their City functions (Seattle)

Commented [PM56]: Again what is the purpose of this section?

VI. Agency Exemptions

- (a) This policy does not apply to the following agencies (eg. Municipal Court, Public Library, the Housing Agency) (Nashville, Seattle)

Commented [PM57]: Again purpose of this section? Exemption? Why exempt the library and housing?

Commented [AH58]: FROM VIC WAHL

Do we know how these agencies ended up being exempted in these cities?

7. Sensitive Information and Data

I. Definitions

Surveillance technology may be of a sensitive or confidential nature. Departments that have such technology can utilize an alternative approval process.

Commented [PM59]: Does this mean then they don't need to comply with all of the above?

II. Approval

Prior to purchasing, installing, accepting funds or donations or entering into agreements to share surveillance technology a Department may initiate an approval process by notifying the Sensitive Surveillance Technology Oversight Board.

- (a) The Sensitive Surveillance Technology Oversight Board members will include the following individuals: the Mayor, the Common Council President, the Chief Information Officer.
- (b) The Department requesting approval for sensitive surveillance technology will present all of the information required for Council approval including a description of the technology, a surveillance technology use policy and a data management policy to the SSTOB for consideration.
- (c) The Department will also provide an explanation for why the technology cannot be approved through the public process.
- (d) The SSTOB will evaluate the proposal and make a determination regarding approval within 30 days of a complete application.
- (e) The Department will provide an annual report on impacts and usage of the sensitive surveillance technology to the SSTOB for each type of tech.
- (f) The SSTOB can determine whether or not a technology is sensitive and qualifies for this approval process.
- (g) The SSTOB can revoke approval for a surveillance technology at any time.
- (h) The CIO will maintain the records of all sensitive technology reviewed by the SSTOB.

Commented [PM60]: By creating this board and procedure you are open to open meetings law & open records law. Who "maintains" this?

Commented [AH61]: FROM VIC WAHL

Overall, it strikes me that this draft and the process thus far has been focused on what other jurisdictions have done and working off their ordinances, rather than starting with what we are trying to accomplish in Madison and using that as our starting point. If the goals are to 1) be sure that the public knows about surveillance technology in use by City agencies (or in the case of sensitive technologies, the public knows that the mayor/council president know); and 2) to have some oversight and assurance that the technologies are being used appropriately; then I think the draft goes way beyond that...