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" shall mean 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.

II. Surveillance technology includes technology who's primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.

i. Additionally, "Surveillance technology" includes, but is not limited to: (a) international mobile subscriber identity (IMSI) catchers and other cell site simulators; (b) automatic license plate readers; (c) electronic toll readers; (d) closed-circuit television cameras; (e) biometric surveillance technology, including facial, voice, iris, and gait-recognition software and databases; (f) mobile DNA capture technology; (g) gunshot detection and location hardware and services; (h) x-ray vans; (i) video and audio monitoring and/or recording technology, such as surveillance cameras, wide-angle cameras, and wearable body cameras; (j) surveillance enabled or capable lightbulbs or light fixtures; (k) tools, including software and hardware, used to gain unauthorized access to a computer, computer service, or computer network; (l) social media monitoring software; (m) through-the-wall radar or similar imaging technology; (n) passive scanners of radio networks; (o) long-range Bluetooth and other wireless-scanning devices; (p) radio-frequency I.D. (RFID) scanners; and (q) software designed to integrate or analyze data from Surveillance Technology, including surveillance target tracking and predictive policing software.

ii. "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; and (f) manually-operated technological devices that are used primarily for internal municipal entity communications and are not designed to surreptitiously collect surveillance data, such as radios and email systems. (Nashville)

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)

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)

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)

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)

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)

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)

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)

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.

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)

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)

IV. The Chief Tech Officer shall direct any City department out of compliance with the ordinance to cease use of surveillance tech

V. A person who is surveilled and injured by a violation of the ordinance my institute proceedings against the City

VI. Departments may use existing technology as long as they comply with the Ordinance

VII. The Executive shall establish a process for determining whether technology is surveillance technology.

VIII. The Council may at any time designate that a technology is or is not surveillance technology. (Seattle)

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.

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)

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)

V. City Functions

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

VI. Agency Exemptions

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

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.

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.