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.

i. "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)

II. "Surveillance data" shall mean any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by surveillance equipment. (Seattle)

III. "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) Description of the purpose and proposed use of the technology,

(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, 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. Notify public

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 and Accountability 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)

II. Enforcement

i. 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.
- (a) 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)

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

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

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

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

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

- Surveillance Use Policy
  - Required when
- Seeking funds
- Seeking funds for surveillance technology including applying or accepting grants, state or federal funds or in-kind or other donations
- Acquiring new technology
- Acquiring new surveillance technology (whether or not money changed hands)
- Using surveillance technology
- Using surveillance technology for a purpose, in a manner, or in a location not previously approved by the Board
- Entering into an agreement with other entities to share equipment or data
- Entering into an agreement with non-County entity to acquire, share or use surveillance technology or information
  - Purpose and Proposed Use of surveillance technology
  - Description of technology
  - 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

- Data Management Policy
  - How data will be collected and retained
  - Who will have access to the data and information
  - Compliance/audit protocols
  - Data retention time frames, destruction protocols
  - Methods for storing data including metadata
  - Individuals/positions that would have access to the data
  - Individuals positions that would ensure compliance

- Exemptions
    - Conditions for Exemption
    - Agencies exempted
        - Under certain conditions
        - Temporary
        - Exigent
    - Requirements law enforcement agencies must meet
        - Approval process
        - Announce planned request
        - Notify public
        - Conduct public engagement
        - Incorporate public comment into planned request
        - Submit request to Council
        - Council reviews
            - Conditions for approval
        - Annual reporting process
            - Surveillance Equipment Report
            - Surveillance Use Policy
            - Data Management Policy
            - Audit
- Sensitive Information and Data
    - Definitions
    - Oversight
    - Reporting
    - Accountability