CM Kitchen MOTION SHEET

Amendment to Resolution regarding License Plate Reader Program

Motion: I move to amend the resolution as follows:

Lines 63 to 65 – see added language:
The City Council directs the City Manager to re-evaluate the Austin Police Department's former policy and/or procedure on license plate readers; develop revisions in collaboration with the Office of Police Oversight and coordinate a minimum of two community input sessions and two meetings with the Public Safety Commission related to the policy. . .

Line 72 – see added language:
. . .may be stored in a criminal case folder for that case or investigation for longer periods as needed. . .

Line 76 to 79 – see added language:
Data sharing will only occur for APD investigating and/or prosecuting criminal activity. If a circumstance arises where the City is required by state or federal law to share the information at the request of a state or federal agency for another law enforcement purpose, then APD will not grant direct access to the database, but will supply the requested information for a specific case or investigation. If the City receives a request for information that is broader than a specific case or investigation, then APD will report that request to the Office of Police Oversight, Mayor and Council prior to sharing any information.

Line 88 – see added language:
…information obtained by the audit and review will be shared with the Office of Police Oversight, and the Public Safety Committee and the Public Safety Commission.

Line 94 – delete "solely":
No person will be the subject of police action solely because of actual or perceived race, color, religion, creed, sex…

Line 103 – add the following:

CM Kitchen MOTION SHEET

The license plate reader data collected by the Austin Police Department will not be used for the purpose of investigations related to immigration status or access to reproductive health services.

Add an Item #8 to the 3rd Be It Resolved:

8. Best practice data security provisions including, but not limited to:
- Role-based access to limit database access to specific officers who must sign an agreement to operate within policies subject to disciplinary action;
- Designation of a Security Officer with responsibility for receiving daily alerts on attempts to log in and/or access data that is not permitted, and for regularly monitoring access to data stored under this provision; and
- Other best practice provisions related to data security for data storage, including the most secure options available for maintaining data.

The City Manager is directed to consult with the City of Austin Security Officer in the development of these provisions.