

COMMISSION RECOMMENDATION

TECHNOLOGY COMMISSION

RECOMMENDATION NUMBER: 20250910-004

Regarding: Recommendation for Establishing Community Input and Technology Commission Review for Sensitive Technology Contracts

WHEREAS, the City of Austin has entered into contracts for technologies involving surveillance and artificial intelligence (AI), including but not limited to mobile security cameras and automated license plate readers, with significant implications for civil liberties, data privacy, and public trust; and

WHEREAS, past contracts, such as the Parks and Recreation Department's mobile surveillance trailer expansion and the Austin Police Department's Automated License Plate Reader (ALPR) agreement with Flock Safety, have revealed risks including unclear data retention practices, insufficient contract safeguards against unauthorized data sharing, and gaps in transparency and accountability; and

WHEREAS, community stakeholders have expressed concerns that sensitive technology contracts have been approved without sufficient public engagement, proactive input from relevant commissions, or rigorous independent review of privacy, security, and ethical considerations; and

WHEREAS, the Technology Commission is charged with advising City Council on issues of technology access, equity, and the ethical use of emerging technologies, including AI and surveillance systems;

NOW, THEREFORE, BE IT RESOLVED, that the Technology Commission recommends that the Austin City Council adopt a formal process to require:

1. **Early Notification & Transparency** – Public posting and notification to relevant commissions prior to Council consideration of any proposed contract involving surveillance technology, automated decision-making systems, artificial intelligence, or other sensitive data-driven technologies.
2. **Commission Review & Recommendation** – Formal referral of such proposed contracts to the Technology Commission (and, where appropriate, the Public Safety Commission or other relevant bodies) for review and recommendations to provide input to Council action.
3. **Community Engagement** – At least one public forum, listening session, or opportunity for stakeholder input before Council approval of sensitive technology contracts.
4. **Contract Safeguards** – Inclusion of clear provisions in contracts to ensure:

- Clear, auditable, and reportable safety mechanisms to protect citizen data and metadata while in vendor custody, tools, systems, or storage, including vendor service providers / cloud providers
 - strict limitations on data retention and sharing, consistent with Council policy,
 - clear definitions of personally identifiable information (PII),
 - independent audit and reporting requirements, and
 - mechanisms for community oversight
 - ability to register complaints and misuse of AI technology
 - remuneration in the event of a breach, data loss, ransomware attack, or other circumstances of compromised data or security as related to citizen data or city data
 - data deletion policy for data no longer needed for its original contracted core purpose, or a way for citizens to remove their identifiable data
 - upon request, provide city representatives ability to validate collected data from citizens in the area, and access to records proving deleted records are fully removed
5. **Ongoing Accountability** – Regular reporting to Council and the public on usage, compliance with policy, and impacts of deployed technologies, with audits conducted by the Office of the City Auditor or other independent body.
6. **Establishing Prohibited Uses** - Working with the Technology Commission and the city's law department, the City Council and/or City Manager will create a list of prohibited uses both for city owned technology and for 3rd party vendor technology. This list will use state laws like TDPSA and TRAIGA as reference, as well as existing city regulations and prohibitions around things like the usage of facial recognition technology, to establish a set of criteria under which a proposed technology contract must be immediately rejected if the proposed deployment involves a prohibited use.

BE IT FURTHER RESOLVED, that this process be applied not only to law enforcement technologies but to all City departments considering contracts involving surveillance, AI, or sensitive data collection, to protect public trust, equity, and civil liberties.

Date of Approval: September 10th, 2025

Record of Vote: Motion to approve this recommendation made by Commissioner Heritage and seconded by Commissioner Pribic. The recommendation was approved on a vote of 7-0.

Attest: 
 Dan Martinez
 Community Technology Division
 Economic Development Department/City of Austin