



Sign-on Letter Against AI Surveillance Cameras in Austin Parks & Pools

Dear Austin City Council Members,

We, the undersigned reproductive justice, civil liberties & human rights, immigration, labor, housing, environmental, and faith organizations, urge you against any resolution that would implement Artificial Intelligence surveillance cameras in Austin city parks and pools.

Austin City Council previously considered [Item 33](#) and is now considering [Item 3](#) which proposes a contract with vendor LiveView Technologies to install AI security cameras in Austin parks and pools, purportedly based on data showing a decrease in crime at pilot locations where security cameras were installed previously. Specific locations of cameras were not specified in the original proposal, nor were details provided with respect to how cameras would be used or which city departments would be granted access to camera footage.

We share concerns about how these cameras may lead to the increased unjust criminalization of communities of color and unhoused neighbors in Austin.

While the harm of property loss and damage arising from car break-ins is an important problem to address, we remain concerned about the more significant types of harm that could arise from caches of data being collected tracking the locations of individuals without their consent, data which would be hackable by bad actors seeking to harm people or obtainable by ICE to facilitate mass deportations. Data collected is data that can be misused or leaked. As we have seen time and time again from large scale data leaks, as data is collected it becomes increasingly valuable - no amount of policy or safeguards will ever completely remove the risk of data theft or security systems being compromised by bad actors.

We are also concerned about the potential for data about our movements to be shared without our consent through this technology. Even if the proposal's claims that no data sharing will occur were accurate, a claim towards which this coalition will always remain skeptical based on a robust body of experience and examples, there is still some kind of machine learning happening on these devices with an on-device record-saving database.

The proposed resolution permits data to be held for 60 days before deletion, an unnecessarily long period offering too broad a window of opportunity for data to be exploited by bad actors.

Further, "delete" is not defined in the contract - if we can not confirm that deletion is independently auditable, then we have no assurance that our data has not merely been copied to another server for LiveView's use as a data broker whose profit model relies on the selling of data harvested from such systems, or for use to train AI models with which we fundamentally take issue.



We have already seen similar AI surveillance companies like Flock lie about the deletion of data harvested by AI surveillance tech, and we should not be fooled here.

Crucially, the AI capabilities of this technology make it fundamentally distinct from typical security cameras. The vendor claims the cameras contemplated in this contract have no AI capabilities and that the features advertised on the website don't apply to this equipment; however, we have concerns that AI features are still available on the models and the company merely "disables" them with vendor SAAS lockouts. Unless the devices are *incapable of object recognition at the hardware level* or, at the bare minimum, the code actually isn't present on device as opposed to a vendor database feature flag, such reassurances don't inspire much confidence.

Put another way - even if we theoretically do not apply the most harmful of these invasive and likely unconstitutional AI surveillance technologies in this contract as currently proposed, once this physical infrastructure exists, there is no way to fully prevent future applications of the tech we oppose following the conclusion of this contract. For example, while the proposed contract states that the system will not use facial recognition, there is no guarantee that at a later date facial recognition technologies will not be applied to the data collected by this system, or integrated into future contracts. Function creep is not merely a concern in the AI surveillance tech space, it is the modus operandi of many of these companies, and we have no reason to doubt that it will occur here.

The proposed contract states that personally identifiable information such as faces or license plates will be "excluded or redacted when not relevant to property crime investigations", however it leaves to the imagination what "when not relevant" actually means. Anything can be reframed by law enforcement as relevant to a criminal investigation or emergency situation.

Further, there have been repeated instances across the country of police abusing their access to such datasets to stalk their partners or harass innocent people. When last year's audit of our Automated License Plate Reader pilot program showed 1 of every 5 APD searches of ALPR data were done without a stated investigative purpose in violation of policy, Austin City Council made no effort to follow up on these improper searches of data to investigate why they occurred. We do not trust that the data collected will be properly used, and we do not trust Austin City Council to do any due diligence to ensure the provisions of this contract will actually be followed.

The proposed contract contains no language explicitly stating that in the event of a violation of the contract's terms on LVT's part, that the company would owe damages to the City or that any consequences would occur at all. Without such deterring language, the legal agreement has no enforcement mechanism and is meaningless.



We know that the Trump administration is actively using data collected by mass surveillance technologies like LiveView cameras to facilitate mass deportations, to hunt abortion seekers, and to track political protesters. In many cases, police are sharing data with ICE and other federal agencies *regardless of the law*.

With recent news stories illuminating alarming collaboration between the Austin Police Department and ICE, we do not want to add to the datasets that create vulnerabilities for our immigrant neighbors and others who may be targeted. We maintain that if data is collected, ICE can go to the parent company to obtain the data, or the Governor could compel the city to share data with ICE. Further, the vulnerabilities of these cameras are so profound that there is nothing materially preventing ICE from going to the physical device to simply download data with a USB.

Parks belong to the people. Mass surveillance in public parks creates a chilling effect, especially in a political climate like this one. Our public spaces are sites of rest, play, and leisure, but they are also sites of protest and organizing in our communities. We all have a right to be in parks without surveillance. We do not want to see the right to privacy become a privilege of the rich, and we urge you not to allow our city to become a testing ground for this invasive technology.

Signed,

The No ALPRs Coalition
Austin Justice Coalition
League of Women Voters of the Austin Area
Ground Game Texas
Texas Unitarian Universalist Justice Ministry (TXUUJM)
Grassroots Leadership
Hands Off Central TX
Texas Civil Rights Project
Workers Defense Action Fund
Austin Sanctuary Network
AAUL
Equity Action
Nonviolent Austin
Austin for Palestine Coalition
Avow Texas

*Please leave a comment with your org name to sign yourself onto the open letter!