

Surveillance Committee Interim Report

October 3, 2026

Table of Contents

Introduction.....	1
Commonly Held Principles.....	2
Committee Impressions of the UA Surveillance Architecture.....	2
Centralized Hub vs. Decentralized Assets (RTCC & UVMS).....	2
Procurement Gaps and “Black Box” Contracting.....	3
Physical & Unmanned Surveillance Expansion.....	3
Evidence from Data & External Investigations: UA Technology Uses.....	3
Empirical Insights from UAPD Search Logs.....	4
Vague Search Justifications:.....	4
Surveillance of Civic Activity:.....	4
Targeted Personal Inquiries:.....	4
Network-Wide Ingress/Egress Exposure:.....	4
Inter-Agency & Out-of-State Access:.....	4
Remaining Attentive to External Precedent Cases.....	4
Out-of-State Extraterritorial Targeting (Reproductive Health & Civil Rights).....	5
Federalization of Local Data & Dragnet Surveillance.....	5
Misuse of Administrative & Surveillance Tools.....	5
Recommendations for Future Work.....	5
Appendix: Comprehensive List of Open Committee Questions.....	6
A. Flock Safety & ALPR Systems.....	6
B. Real Time Coordination Center (RTCC) & Data Architecture.....	6
C. Inter-Agency Data Sharing & External Networks.....	7
D. Unmanned Aerial Vehicles (UAVs) & Emerging Tech.....	7

Introduction

The University of Arizona has long claimed a commitment to creating a safe and secure environment for all members of our diverse community, including students, faculty, staff, and visitors. Over recent years, and especially in the aftermath of the publication of [the Pax report](#) in early 2023, significant progress has been made through the creation of [the Office of Public Safety \(OPS\)](#) and efforts at coordination between OPS and various campus departments to establish comprehensive security protocols and systems. These initiatives are necessary in building a campus culture where safety and security are integrated thoughtfully into our shared spaces

Surveillance systems represent a powerful but potentially abused tool within this broader public safety mandate. Video monitoring, access controls, and related technologies serve as complements to community partnerships, emergency response planning, and preventive education. However, because surveillance systems intersect with fundamental questions about privacy, data management, fiscal decision-making, and institutional oversight, they merit dedicated examination and transparent communication with the campus community, as well as legal guardrails and guidelines on their use.

This interim report has been prepared by a faculty-led committee charged by Chair of Faculty, Prof. Leila Hudson, with evaluating the University's existing surveillance systems. This committee was convened in November 2025 after the issue of Flock's automated license plate readers (ALPRS) on campus was introduced to Faculty Senate on 6 October 2025. The committee members were nominated by the Nominating Committee and by snowball techniques and the Staff Council nominated a member of staff. After the withdrawal of the initial committee chair due to conflicting obligations, Chair of the Faculty Leila Hudson stepped in as acting committee chair.

Our committee shares the foundational goals of the Office of Public Safety: to help ensure the safety and security of all stakeholders on our campus. We recognize that effective public safety is essential to our mission as an educational institution and to the well-being of our community and also that surveillance systems themselves can represent a threat to safety, privacy, and constitutional freedoms.

This report serves two primary purposes. First, it is intended to provide all campus stakeholders with transparent information about how surveillance systems are currently being managed, their scope and capabilities, and the oversight mechanisms in place to govern their use. Second, it provides an opportunity for faculty input into the ongoing process of evaluating and refining campus surveillance infrastructure. This input reflects both academic perspectives on privacy, ethics, and institutional governance, and practical insights from those who work daily within our campus environment.

We believe that this collaborative approach to examining our surveillance systems reinforces the University's commitment to balancing safety with the values of transparency and accountability that define our academic community. The committee believes it is important to situate

surveillance practices at the University of Arizona in historical and political context. The final report will offer a useful definition of surveillance and sketch out the legal parameters of surveillance before looking specifically at surveillance on university campuses. Comparing UA surveillance practices with those of its peer institutions will help us identify best practices and areas of concern.

Scope of Committee and Report

The Ad Hoc General Faculty Committee on Campus Surveillance has been tasked with identifying physical surveillance systems on campus and their related physical, digital, and organizational infrastructure, investigating these systems in light of relevant University/government guidelines and community feedback, and recommending policies and best practices for use of these systems to address both public safety and civil rights concerns. This report provides an overview of our activities to date. Thus far, we have engaged with several major actors on campus regarding their use of physical surveillance and related infrastructure. This engagement has included an exploration of shared principles related to surveillance use as a starting point to an ongoing conversation, inquiry about the information currently available on surveillance systems and practices, and the pursuit of additional information on this topic. Going forward, we will continue to engage with campus stakeholders, seek answers to questions raised by our inquiry to date, and pursue additional collaboration and participation opportunities. The questions that we will be asking of ourselves and others are provided in an appendix to this report.

Commonly Held Principles

Managing public safety across a 400-acre campus hosting over 50,000 daily visitors presents complex operational challenges. Our committee's inquiry is anchored in several foundational principles we assume are commonly held across shared governance and university leadership:

- *Shared Commitment to Campus Safety*: Effective public safety is indispensable to the university's academic, research, and community missions.
- *Balancing Security with Constitutional Freedoms*: Surveillance tools are not inherently neutral; their application must strictly respect constitutional protections, including First Amendment rights to free speech/assembly and Fourth Amendment protections against unreasonable searches and dragnet surveillance.
- *Transparency and Sunshine in Governance*: Decisions surrounding technology acquisition, data retention, vendor contracting, and inter-agency data sharing must occur in the open, with meaningful input from shared governance (Faculty Senate, Staff Council, student government) rather than post-hoc administrative notifications.
- *Independent Oversight and Accountability*: Internal self-auditing by law enforcement or public safety units is insufficient to build institutional trust. Accountability requires clear, standardized logging, independent auditing, and transparent public reporting.
- *Protection of Vulnerable Populations*: Campus security practices must actively prevent harm to community members who may be targeted by outside jurisdictions or external

entities (e.g., regarding civil immigration enforcement or access to reproductive healthcare).

- *Fiscal Stewardship*: Decisions to purchase technology and commit university funds to long-term software and hardware contracts with external vendors should include substantive stakeholder input on the necessity of expenditures relative to their anticipated function.

Committee Impressions of the UA Surveillance Architecture

Based on site visits (including Spring 2026 visits to the Real Time Coordination Center), meetings with Procurement, and reviews of public safety documentation, the committee has formed the following impressions regarding the University's current setup:

Centralized Hub vs. Decentralized Assets (RTCC & UVMS)

- The Real Time Coordination Center (RTCC) (located in the Administration Building basement) serves as the primary hub for unified campus safety operations.
- Video monitoring across campus is integrated via the University of Arizona Video Management System (UVMS), co-administered by OPS and UITS under the interim *Security Camera Policy* (which explicitly carves out exceptions for UAPD cameras, drones, and ALPRs).
- Operational Impressions: While centralized monitoring dramatically improves emergency response times and officer deployment efficiency, oversight mechanisms across connected platforms are highly fragmented. Auditing capabilities vary widely between systems. Some offer robust user logging, while legacy platforms appear not to offer any kind of audit trail.

Procurement Gaps and “Black Box” Contracting

- Inquiries with Procurement leadership revealed that they (UA procurement) can neither search their databases easily nor produce a list of the vendors/companies with whom UA contract cloud storage.
- Operational Impression: The lack of accessible vendor contract data presents a potential blind spot regarding data ownership, third-party data broker access, off-shoring/off-site storage policies, vendor AI training rights, and total operational spend.

Physical & Unmanned Surveillance Expansion

- Flock Safety ALPRs: The University of Arizona is one of more than 150 institutions of Higher Education using Flock's surveillance technology network.¹ UAPD operates 63 Flock Falcon ALPR cameras situated around the campus perimeter and key internal

¹ Monahan, T. (2026). Flock on campus: university police as appendages of a national policing apparatus. *Policing and Society*, 1–23. <https://doi.org/10.1080/10439463.2026.2702635>

arteries (e.g., West Mall, Sixth Ave, Highland Ave). Network settings were shifted on November 4, 2025, from a “National Lookup” default to a “State Lookup” default, which facilitates reciprocal access across 69 state entities.

- Unmanned Aerial Vehicles (UAVs): The deployment of drones by UAPD represents a rapid, recent capability expansion. The committee noted a critical absence of established protocols governing drone flight waivers, crowd monitoring under First Amendment protections, and privacy/HIPAA safeguards for recorded aerial footage.

Evidence from Data & External Investigations: UA Technology Uses

Much of the empirical data detailing how UA's surveillance infrastructure is utilized comes from public record requests through the Freedom of Information Act (FOIA) and external data aggregators (such as [HavelBeenFlocked.com](https://havelbeenflocked.com)), which indexed UAPD's search logs during its participation in the national Flock network prior to November 4, 2025.

Empirical Insights from UAPD Search Logs

Vague Search Justifications:

- Excluding formal case numbers, the single most frequent search reason logged by UAPD officers on the national database was the two-letter acronym, “CI” (criminal investigation).
- System logs lack granular context, raising questions about whether standard National Incident-Based Reporting System (NIBRS)-based crime category drop-down requirements were historically enforced.

Surveillance of Civic Activity:

- Public logs reveal multiple instances where searches were conducted on the national database (which includes the UAPD database) by external (non-UA) agencies under the explicit search reason “demonstration” or “protest.”

Targeted Personal Inquiries:

- At least one UAPD search of the national database explicitly listed the personal name of an individual engaged in active litigation against the University of Arizona.

Network-Wide Ingress/Egress Exposure:

- Fixed perimeter ALPRs capture thousands of non-university commuters daily along public thoroughfares (e.g., Sixth Avenue and Highland Avenue).

Inter-Agency & Out-of-State Access:

- While UAPD transitioned off National Lookup in late 2025, search logs show that out-of-state entities previously queried UAPD's database freely. Furthermore, UAPD maintains direct informal and formal data-sharing pathways with local law enforcement (e.g., TPD) and federal partners who may participate in broader national networks or [287\(g\) agreements](#), potentially enabling federal agencies access to the search network via local agency partners.

Remaining Attentive to External Precedent Cases

To prevent abuses and guard against systemic failure, the University of Arizona must evaluate real-world risks demonstrated in other jurisdictions. To be clear, there is no evidence that similar actions or events have occurred at the University of Arizona. To be sure, we assume that the UA is actively guarding against any such occurrences taking place locally.

Out-of-State Extraterritorial Targeting (Reproductive Health & Civil Rights)

- External Precedent: In other U.S. jurisdictions, evidence has emerged that law enforcement agencies in states with strict reproductive bans have leveraged national ALPR networks to track individuals traveling across state lines for reproductive healthcare.²
- UA Vulnerability: While UAPD's internal FAQ prohibits using ALPR data to monitor reproductive healthcare or civil immigration status, it is not clear to us that UAPD has toggled on Flock's software-level filters that automatically block queries related to immigration or reproductive care, nor has it toggled restrictions on federal database access.³

Federalization of Local Data & Dragnet Surveillance

- External Precedent: Emerging practices across the Flock network at institutions of Higher Education point towards the potential for rapid federalization of municipal and campus data through centralized intelligence hubs or broad subpoena powers, which runs the risk of overriding local administrative policies.⁴

² See discussion of case in Texas:

<https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-mis-sing-person-it>

³ See discussions of these Flock system capabilities:

<https://www.flocksafety.com/blog/flock-aligns-license-plate-reader-technology-with-state-specific-legal-frameworks> and

<https://www.flocksafety.com/blog/flock-guardrails-address-lpr-privacy-concerns-and-police-transparency>

⁴ For discussion of the prospective concern that Flock could turn campus police departments into appendages of a national policing apparatus see Monahan (2026).

- **UA Vulnerability:** In an environment of expanding executive law enforcement powers, the claim that the university “owns its data” is fragile if vendors (or university units) are compelled to hand over dragnet surveillance feeds without clear legal defense mechanisms or public notification.

Misuse of Administrative & Surveillance Tools

- **External Precedent:** Documented law enforcement misuses of ALPR and video monitoring system networks nationwide include pretextual stops based on false system reads, stalking/tracking of romantic partners, and unconstitutional monitoring of political dissidents.⁵
- **UA Vulnerability:** UAPD noted in April 2026 meetings that logging individual instances of data sharing with outside agencies was “not practical,” conflicting directly with written UAPD policy and disabling a core mechanism required to detect and remediate misuse.

Recommendations for Future Work

To transition from reactive inquiry to proactive, values-aligned governance, the committee recommends:

1. **Institutionalized Shared Governance Oversight:** Establish a permanent, joint Faculty Senate, Staff Council, and Student Government standing committee with explicit opportunity to provide feedback regarding public safety technology adoptions and policy updates.
2. **Ground-Up Policy Drafting:** Ask that all future surveillance, camera, and data retention policies be co-created via open shared governance processes, avoiding top-down administrative policy rollouts.
3. **Independent Audit Protocols:** Replace self-auditing models with independent oversight to review RTCC access, ALPR search logs, and Threat Assessment Management Team (TAMT) technology requests.
4. **Cost-Benefit & Non-Material Impact Analyses:** Conduct comprehensive financial audits detailing all direct and indirect expenses (contracts, server costs, personnel, TAMT, RTCC) alongside studies analyzing how continuous public surveillance affects campus culture, academic freedom, and community trust.
5. **Clear Protocol on Email & Digital Monitoring:** Clarify the committee's scope to address emerging digital monitoring policies, including recent updates to university email surveillance rules.

Appendix: Comprehensive List of Open Committee Questions

⁵ See reporting on series of cases:

<https://www.washingtonpost.com/technology/2026/08/02/how-police-officers-used-vast-network-cameras-spy-their-exes/>

A. Flock Safety & ALPR Systems

1. What technical safeguards exist within the Flock user interface to detect, flag, or prevent search misuse?
2. What specific administrative safeguards has UAPD instituted internally to remediate improper searches?
3. Why are available Flock software filters for reproductive health, immigration enforcement, and federal access restrictions currently untoggled/unutilized by UAPD?
4. Which local or state LEAs outside the Flock State Network hold direct, indirect, or manual access to UAPD's ALPR feeds, and how is this access logged?
5. What is UAPD's official protocol if Flock Safety is legally compelled to grant unrestricted federal access to university-generated data?
6. Are all federal requests for ALPR data logging and record sharing systematically archived and made available for governance review?
7. Has UAPD evaluated localized, non-cloud ALPR alternatives (e.g., ReKor, Eufy) that keep data strictly on-premises?

B. Real Time Coordination Center (RTCC) & Data Architecture

8. What complete set of platforms feeds into or pulls data from the RTCC (e.g., 911 logs, VMS feeds, CatCard access, point-of-sale data, Wi-Fi location metrics, Symplicity/Advocate)?
9. What specific university entities approve access to internal data networks, and what legal/administrative threshold (e.g., "reasonable suspicion") is required?
10. How does the Threat Assessment Management Team (TAMT) interact with the RTCC, what due process/appeal channels exist for flagged individuals, and how are TAMT directives logged?
11. How long are raw video, aerial, and metadata logs retained across systems, and what are the precise procedures for scheduled data destruction?
12. What specific software or integration platforms synthesize disparate VMS networks into the UVMS?
13. What reporting logs are regularly produced by the RTCC, and through what public or shared governance mechanisms can they be accessed?

C. Inter-Agency Data Sharing & External Networks

14. Is UAPD an active partner in the Homeland Security Information Network (HSIN) or RISSIntel? Does RISSIntel have direct access to UA surveillance databases?
15. What formal or informal data-sharing agreements exist with external law enforcement entities (e.g., TPD, Pima County Sheriff, federal agencies), and how are non-AZPOST training standards accounted for?
16. How does the university audit downstream data sharing (e.g., secondary sharing by partner agencies under 287(g) agreements)?

D. Unmanned Aerial Vehicles (UAVs) & Emerging Tech

17. Who pilots UAPD drones, what flight certifications/waivers are held for beyond-line-of-sight operations, and what training covers First Amendment protections during crowd monitoring?
18. Where is aerial videographic data archived, and what specific technical measures prevent HIPAA violations when drones capture medical or health-crisis incidents?
19. What formal Technology Adoption Policy governs OPS/UAPD when evaluating, piloting, or deploying newly emerging surveillance tech?