TO: Harrison Keller (Office of the President)
FROM: Serene Plummer
DATE: March 17, 2026
SUBJECT: Proposal to Restrict Identity-Linked Surveillance at the University of North Texas

---

Qualification

I am currently a Computer Science student at the University of North Texas, focusing on software engineering and artificial intelligence. My academic background has introduced me to data systems, machine learning, and large-scale analytics platforms that process user behavior and identity-linked data. Because of this, I understand both the technical capabilities and risks associated with surveillance technologies.

In addition to my coursework, I conducted primary and secondary research on surveillance practices in public institutions. This includes an interview with a UNT IT student assistant and a survey of students, as well as an analysis of scholarly and industry sources. This combination allows me to evaluate both the technical and ethical implications of identity-linked surveillance on campus.

Introduction

This proposal addresses the potential expansion of identity-linked pedestrian surveillance at the University of North Texas. These systems can track movement patterns and link that data to individual identities using technologies such as student ID systems or facial recognition. While these tools are often justified as necessary for campus safety, they raise significant concerns about privacy, transparency, and ethical AI use.

The purpose of this proposal is to recommend clear policy restrictions that limit how surveillance technologies are used at UNT. My interest in this issue developed through my research into AI systems, as well as findings from my interview and survey. As a student directly affected by these systems, I believe it is necessary to ensure that safety measures do not result in unnecessary or invasive monitoring.

Current Situation / Problem

Based on my interview, current surveillance practices at UNT are primarily focused on cybersecurity and access control. Systems such as laptop monitoring and key fob entry are used

to protect students and restrict access to certain buildings. These practices are generally justified as necessary for safety and operational security.

However, the infrastructure to link identity to movement already exists. Student ID systems and access control mechanisms demonstrate that individuals can already be tracked in specific contexts. While this tracking is currently limited, there are no clearly defined policies preventing the expansion of these systems into broader identity-linked surveillance.

My secondary research further supports this concern. According to the American Civil Liberties Union, surveillance technologies are often implemented before strong policies are established, allowing systems to expand over time without proper oversight. Similarly, the Electronic Frontier Foundation highlights how institutions frequently use advanced monitoring tools without fully informing students, creating a lack of transparency.

Research also shows that these technologies can negatively impact student behavior. Surveillance has been linked to a "chilling effect," where individuals change how they act or express themselves because they know they are being monitored. In a university setting, this directly conflicts with the purpose of higher education, which is to encourage open discussion and critical thinking.

Additionally, partnerships with private companies such as Palantir Technologies introduce further risks. These companies provide powerful data analytics tools, but their systems often lack transparency, making it difficult to determine how data is processed or used. This creates concerns about accountability and long-term data security.

Without clear limitations, surveillance technologies at UNT could expand beyond their original purpose, increasing the risk of misuse and reducing student trust.

Project Plan

To address these issues, I propose implementing policy restrictions that limit identity-linked surveillance while still maintaining campus safety. This proposal is based on my interview, survey data, and secondary research.

Restrict Surveillance to Emergencies Only

Surveillance systems should only be used in situations involving immediate threats, like active violence or serious crimes. This keeps surveillance focused on actual safety concerns instead of being used all the time.

Eliminate Identity-Linked Tracking

UNT should not allow systems that connect movement or behavior directly to individual identities. This includes limiting facial recognition and making sure movement tracking is not tied to student IDs or personal data.

Limit Long-Term Data Collection and Profiling
UNT should also prevent the creation of long-term databases that track and build profiles on students over time. Surveillance data should not be used to analyze behavior patterns or predict actions. Any data that is collected should be minimal and only kept for a short period of time unless it is needed for an active investigation.

Keep Data Within the University
All surveillance data should stay within UNT systems. It should not be shared with or stored by outside companies. This helps prevent third parties from collecting or using student data and keeps everything under university control.

Increase Transparency
Students should be clearly informed when surveillance is being used, what data is being collected, and why. Policies should be easy to find and actually understandable, not hidden in long documents.

Implement Regular Audits
The university should regularly review its surveillance systems to make sure they are not being misused or expanded beyond their original purpose. This helps keep everything accountable.

Strengthen Data Protection Measures
All data should be encrypted and only accessible to authorized personnel. It should not be sold, shared, or used outside of its intended purpose.

Cost Considerations
This proposal mainly focuses on changing policies rather than adding new technology, so it would not be very expensive. It also helps UNT avoid bigger legal or ethical issues in the future, which could cost more in the long run.

Project Benefits

This proposal provides several important benefits across the university community.
For students, these policies protect personal privacy and reduce concerns about constant monitoring. This helps create a more open and comfortable environment for learning and expression.

For the university, adopting ethical AI practices improves transparency and reduces the risk of legal or reputational damage. Clear policies also demonstrate accountability in how student data is handled.

For the broader community, this approach balances safety with individual rights. It ensures that surveillance is used responsibly while setting a standard for ethical technology use in higher education.

Project Timeline

Phase	Task	Date
Phase 1	Draft policy changes	April 2026
Phase 2	Administrative review	May 2026
Phase 3	Implementation	June–July 2026
Phase 4	First audit	Fall 2026

Conclusion

While surveillance technologies can contribute to campus safety, their use must be carefully limited to protect student privacy. The University of North Texas can take a proactive approach by implementing clear policies that restrict identity-linked surveillance and promote ethical AI practices.

These changes are practical, cost-effective, and necessary. They ensure that safety measures remain effective without creating an environment of unnecessary monitoring. By adopting this proposal, UNT can strengthen student trust while setting a strong example for responsible technology use.

Thank you for your time and consideration. If you have any questions or would like further clarification, please feel free to contact me at my UNT email address.

Works Cited (MLA)

American Civil Liberties Union. What's Wrong with Public Video Surveillance? www.aclu.org/documents/whats-wrong-public-video-surveillance

American Civil Liberties Union of Northern California. Fighting High-Tech Government Surveillance. www.aclunorcal.org/fighting-high-tech-government-surveillance

Bell, Kyilee. Personal Interview. 11 Feb. 2026.

Electronic Frontier Foundation. Scholars Under Surveillance: How Campus Police Use High-Tech Tools to Spy on Students. www.eff.org/deeplinks/2021/03/scholars-under-surveillance-how-campus-police-use-high-tech-spy-students

The Guardian. "School Surveillance Tech Raises Privacy Concerns, ACLU Report Finds." 4 Oct. 2023.www.theguardian.com/technology/2023/oct/04/school-surveillance-tech-aclu-report

Qualtrics Survey. "Student Attitudes Toward Identity-Linked Surveillance at UNT." Feb. 2026. https://unt.az1.qualtrics.com/jfe/form/SV_4IpVr6kXeW09T9k

Winston, Ali. "The Data-Mining Company That's Building a Surveillance State." Bloomberg Businessweek, 2018. www.bloomberg.com/features/2018-palantir-peter-thiel/