March 28, 2026

Harrison Keller
Office of the President
University of North Texas
1155 Union Circle
Denton, TX 76203

Dear Dr. Keller,

I am writing to formally submit my report titled *"Restricting Identity-Linked Surveillance at the University of North Texas: A Data-Driven Analysis of Privacy and Safety."* This report expands on my previously approved proposal and evaluates the potential impact of identity-linked surveillance technologies on campus.

The purpose of this report is to examine how surveillance systems that track and link student movement to personal identity may affect privacy, transparency, and trust at UNT. To support this analysis, I conducted an interview with a university-affiliated IT student assistant, distributed a Qualtrics survey to UNT students, and reviewed secondary sources related to artificial intelligence, surveillance, and data ethics.

The findings show that while current surveillance at UNT is mostly focused on security and access control, students are largely uncomfortable with identity-linked tracking and strongly support policies that limit surveillance to emergencies. Based on this, the report recommends restricting identity-linked surveillance, increasing transparency, and implementing clear data protection policies.

Thank you for your time and consideration. Please feel free to contact me if you have any questions regarding this report.

Respectfully,

Serene Plummer
Computer Science Student
SerenePlummer@my.unt.edu

2026

University of North Texas

RESTRICTING IDENTITY-LINKED SURVEILLANCE

A DATA-DRIVEN ANALYSIS OF PRIVACY, ETHICS, AND CAMPUS SAFETY

PREPARED FOR
Center for Cyber and AI Security

PREPARED BY
Serene Plummer

Abstract

This report examines the ethical concerns of identity-linked surveillance at the University of North Texas, where technologies can track and link individual identities to movement data. Mixed-method research, including an interview with an IT assistant and a survey of 22 students, reveals that while current monitoring focuses on security, students are largely unfamiliar with and uncomfortable with identity-linked tracking, expressing strong support for transparency and emergency-only restrictions. Ultimately, the findings suggest that UNT should implement formal policy restrictions to protect student privacy, ensure data anonymity, and maintain institutional trust without compromising campus safety.

Table of Contents

Introduction

Background

The University of North Texas (UNT), like many modern colleges and universities, is increasingly using advanced data analytics and surveillance tools to boost campus security and make operations run more smoothly. While these systems, including platforms developed by companies like Palantir Technologies Inc., offer the potential for better safety, they also introduce significant risks regarding identity-linked pedestrian surveillance. This report examines the ethical and technical impacts of tracking student movement and linking behavior data to individual identities on campus.

The main purpose of this research is to push for a specific policy change: restricting the use of identity-linked surveillance at UNT to emergencies only. Protecting student privacy is essential to maintaining a healthy school environment. Surveillance often creates a "chilling effect," where people change their behavior or hold back on speaking their minds because they know they are being watched. This is particularly harmful in a university setting, which should focus on open discussion and critical thinking.

The importance of this topic lies in the balance between security and individual liberty. As a Computer Science major, I recognize that the technical infrastructure for comprehensive monitoring already exists within UNT's digital systems, such as student ID and access control mechanisms. However, without clear, transparent policies, these systems can expand beyond their intended scope without adequate oversight. This report concludes that implementing strict guidelines for anonymity, transparency, and regular audits is essential to ensuring that UNT remains a safe but private campus for all students and faculty.

Methods

To evaluate the current state of surveillance and student attitudes at the University of North Texas, a mixed-methods research approach was employed. This methodology included primary research through a professional interview and a student eSurvey, as well as secondary research from scholarly and advocacy sources.

Primary Research: Interview and eSurvey

The primary research phase began with an interview conducted on Feb 11th 2026, with a UNT-affiliated IT student assistant. The purpose of this interview was to gain insight into the university's current IT infrastructure, data handling practices, and existing surveillance tools, such as key fob access and laptop monitoring. Detailed written notes and a recording were taken to ensure the accuracy of the technical information provided.

Subsequently, a Qualtrics eSurvey was distributed to UNT students in late February 2026. The survey targeted current undergraduate and graduate students to measure their awareness of

identity-linked tracking and their comfort levels regarding surveillance technologies. Recruitment was handled through Canvas email and class group chats to ensure a sample of active students directly affected by campus policies.

Secondary Research Sources

Comprehensive secondary research was conducted to ground the proposal in established ethical frameworks and industry standards. The following sources provided the foundation for analyzing the risks of data mining and the importance of privacy in public spaces:

- American Civil Liberties Union. *What's Wrong with Public Video Surveillance?* ACLU.
- American Civil Liberties Union of Northern California. *Fighting High-Tech Government Surveillance.*
- Electronic Frontier Foundation. *Scholars Under Surveillance: How Campus Police Use High-Tech Tools to Spy on Students.*
- The Guardian. "School Surveillance Tech Raises Privacy Concerns, ACLU Report Finds."
- Winston, Ali. "The Data-Mining Company That's Building a Surveillance State." Bloomberg Businessweek.

Results

The research findings indicate a significant gap between the university's technical capabilities and student awareness of surveillance policies. Data synthesized from the Qualtrics eSurvey and the IT interview highlight a strong student preference for transparency and for the restricted use of monitoring tools.

eSurvey Data Synthesis

The eSurvey revealed that while students generally support campus safety measures, they are largely uncomfortable with systems that link their physical movement to their personal identity. A majority of respondents expressed that they were previously unaware of the extent to which identity-linked tracking is possible with existing infrastructure.

One clear finding from the survey is that many students are not very familiar with identity-linked surveillance technologies. When asked whether they were familiar with the concept of surveillance systems capable of linking movement data to individual identities, most respondents reported little or no familiarity.

Specifically, 7 respondents reported being "not familiar at all," and 6 reported being only "slightly familiar." Only 5 respondents indicated they were very familiar with the concept.

This lack of awareness suggests that many students may not fully understand the capabilities of modern surveillance technologies or how these systems could potentially be used on college

campuses. Even so, students still expressed strong opinions about privacy concerns once the idea was explained in the survey.

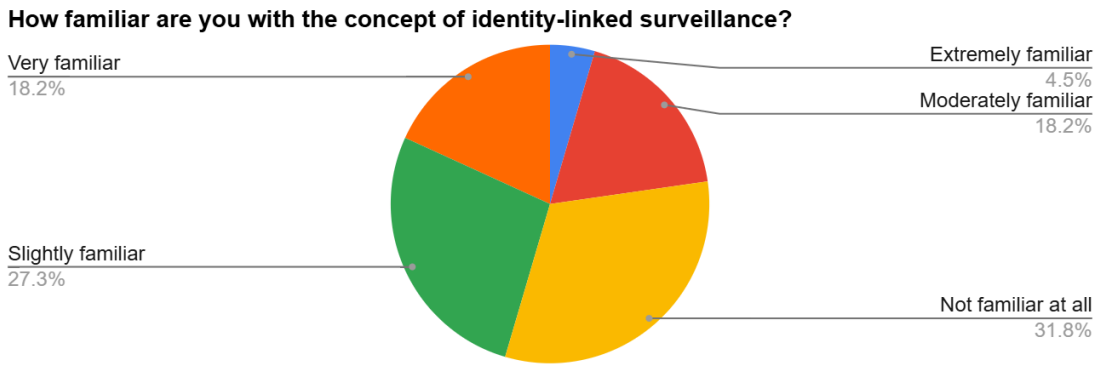

Figure 1: Familiarity with Identity-Linked Surveillance

A second major pattern in the survey results is that students are generally uncomfortable with the idea of identity-linked surveillance being used on campus.

When asked about their comfort level with identity-linked pedestrian surveillance at UNT, 19 out of the 22 respondents expressed discomfort. Out of these, 10 reported being extremely uncomfortable, and 9 reported being somewhat uncomfortable. Only 3 respondents reported feeling neutral, and none reported feeling comfortable with the idea.

These responses suggest that many students see identity-linked surveillance as a possible invasion of privacy. Open-ended responses also supported this concern, with students mentioning fears of "privacy invasion," "being constantly watched," and uncertainty about how their personal data might be used or accessed. Some respondents also raised concerns about possible data misuse or security breaches.

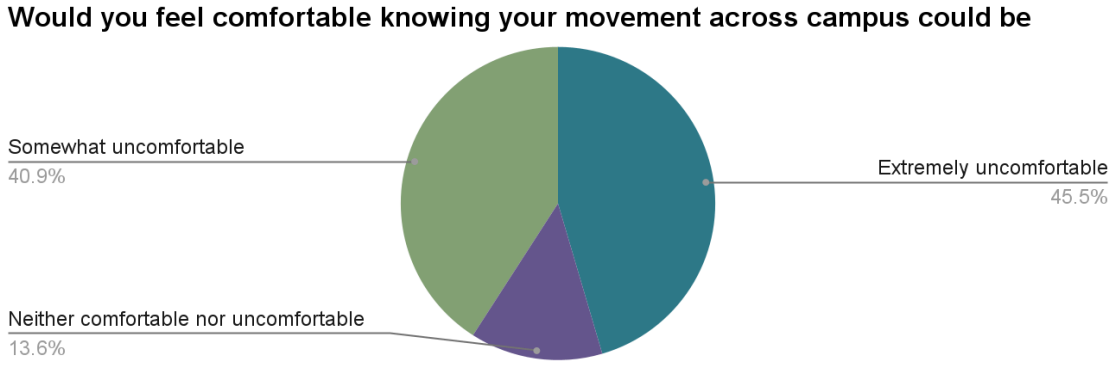

Figure 2: Comfort Level with Identity-Linked Surveillance

The third major finding is that students strongly support clear policies limiting how surveillance technologies are used on campus. Several survey questions showed strong support for transparency, oversight, and restricting surveillance to emergencies.

For example:

13 respondents said surveillance should be limited strictly to emergencies
12 respondents said pedestrian data should remain anonymous by default
18 respondents said students should be notified when surveillance technology is being used
12 respondents supported regular independent audits of AI-based surveillance systems

These results suggest that students are not completely opposed to security technologies, but they want strong safeguards in place to protect their privacy. Many respondents emphasized the importance of transparency, including clear explanations of what data is being collected, who has access to it, and how it is stored.

Open-ended responses also reinforced this point. Several students said they would feel more comfortable if surveillance were limited to safety situations, if data collection practices were clearly explained, and if human oversight were involved.

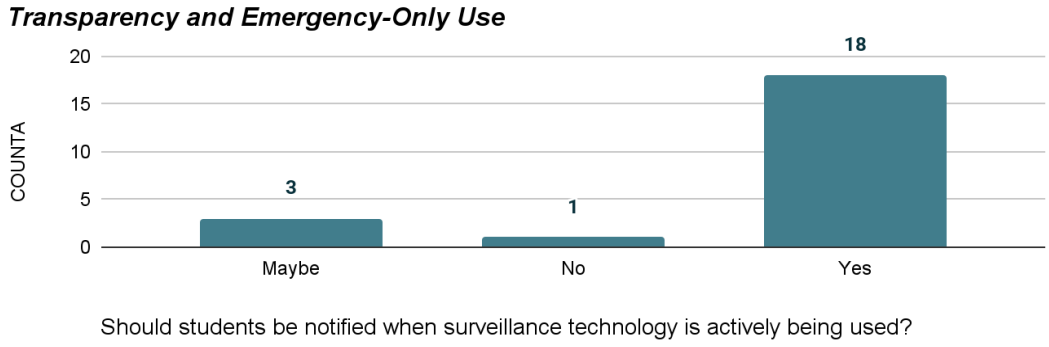

Figure 3: Support for Notification When Surveillance Is Used

Interview and Technical Findings

The interview with the IT student assistant confirmed that UNT already utilizes systems for cybersecurity and access control, such as key fob entries and laptop monitoring in labs. These systems are currently framed as operational safety measures; however, the assistant noted that the infrastructure to link these logs to individual identities exists and could potentially be expanded. This technical reality aligns with secondary research from the ACLU, which suggests that surveillance technology often scales faster than the policies intended to govern it.

Discussion

The results of this study clearly demonstrate that students at the University of North Texas value their privacy and desire a more transparent relationship with campus security technology. The

"heart" of the issue is not whether surveillance should exist, but rather how it is governed and who is protected by its limitations.

The high level of support (18 out of 20 respondents) for notification when surveillance is in use indicates that the current "opaque" nature of campus monitoring is a point of contention. As noted in the EFF research, a lack of transparency creates an environment of distrust. By implementing the proposed "emergency-only" restriction, UNT can realign its security practices with its educational mission. This approach addresses the problem of the "chilling effect" by ensuring that students feel free to participate in campus life without the weight of constant, identity-linked monitoring.

The interview insight regarding existing identity-linking capabilities highlights a critical vulnerability: the lack of a formal policy preventing the expansion of these tools. The RAMifications of allowing companies like Palantir Technologies to manage student data are significant. Such partnerships risk moving sensitive behavioral data outside of university control, where it could be used for profiling rather than safety.

Ultimately, this proposal answers the research question by demonstrating that ethical AI deployment is feasible through policy, not just technology. By mandating anonymity and regular audits, UNT can set a standard for responsible tech use in higher education. This rhetorical argument is supported by the data: safety does not have to come at the expense of identity protection. Implementing these changes would foster a culture of trust and ensure that UNT remains a leader in both innovation and student advocacy.

Conclusion

This research looks at the ethical and technical effects of identity-linked surveillance technologies at the University of North Texas. While existing monitoring systems remain primarily focused on security and access control, the data indicates a major discomfort among the student body regarding identity-linked tracking, alongside overwhelming support for strict policy restrictions and enhanced openness.

In light of these findings, the report recommends a series of specific policy improvements. First, the use of surveillance technologies must be restricted strictly to emergencies involving immediate threats to campus safety. Second, the University should formally ban systems that connect behavioral movement data to individual identities, ensuring that all pedestrian data remains anonymous by default. Third, UNT must increase openness by implementing clear notification rules to inform students when surveillance tools are in operation and precisely what data is being collected.

Furthermore, UNT should establish protections against long-term data keeping and behavioral analysis, ensuring that sensitive information is never utilized beyond its original, intended purpose. To maintain responsibility, the university should implement regular, independent checks to verify following the rules with ethical AI standards and established data protection policies.

Although restricting surveillance capabilities may slightly reduce the university's capacity to address minor non-emergency incidents, the protection of student privacy and the maintenance of institutional trust are most important. By adopting these recommendations, the University of North Texas can keep up a standard of campus safety that does not come at the expense of individual freedom or responsible, ethical technology use.

References

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

Plummer, Serene. *"Student Attitudes Toward Identity-Linked Surveillance at UNT."* Qualtrics Survey. 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/

Appendix

Interview Questions

1. Can you describe your role at UNT and how it relates to campus safety, data systems, or technology use?
2. What types of surveillance or monitoring technologies are currently used on campus to track pedestrian movement or activity, if any?
3. To your knowledge, are any systems capable of linking movement or behavioral data to individual identities, such as student IDs or facial recognition?
4. What are the primary reasons UNT considers or uses surveillance technologies, and how are those decisions justified to students and staff?
5. How does the university currently inform students about when and how monitoring occurs on campus?
6. What safeguards are in place to prevent surveillance data from being misused, overextended, or accessed under false pretenses?
7. In your opinion, where should the line be drawn between necessary security measures and invasive monitoring on a college campus?
8. How does UNT ensure that surveillance technologies comply with ethical AI principles, particularly regarding privacy and consent?
9. What challenges or concerns would arise if UNT limited surveillance technologies strictly to emergencies only?
10. What policy changes or technical limitations do you believe would most effectively protect student privacy while still maintaining campus safety?

eSurvey Questions

1. Classification (Freshman, Sophomore, Junior, Senior, Graduate)
2. Major
3. Do you live on campus? (Yes/No)
4. Before this survey, were you aware that universities can use advanced analytics platforms such as Palantir Technologies Inc. to analyze pedestrian movement data?
5. How familiar are you with the concept of identity-linked surveillance (tracking movement data tied to individual identities)?
6. Would you feel comfortable knowing your movement across campus could be tracked and linked to your identity?
7. Should identity-linked surveillance be limited strictly to emergency situations (e.g., active threats)?
8. Should pedestrian data collected on campus remain anonymous by default?
9. Should students be notified when surveillance technology is actively being used?
10. How much do you trust the University of North Texas to use surveillance data responsibly?

11. Should the university conduct regular independent audits of any AI-based surveillance systems?
12. What concerns, if any, do you have about identity-linked surveillance on campus?
13. What policies would make you feel more comfortable about surveillance technologies being used at UNT?