TRENDS SNAPSHOT

Campus Safety, Technology, and Privacy

Like nearly every other office in higher education, campus-safety departments are awash in opportunities to upgrade their digital tools. A revolution in security technology, driven by both traditional and new artificial-intelligence products, has been embraced by campus-safety leaders.

Those officials report that they are likely to use AI-based tools this academic year to monitor their campuses, control access to buildings, improve their response times, perk up their alert systems, and detect specific threats, such as the presence of weapons or vehicles that have been connected to past crimes.

And because most colleges have already installed advanced technologies, including surveillance cameras, they are well positioned to plug new tools into their existing security platforms. As of last year, 94 percent of higher-ed institutions, K-12 schools, and health-care organizations had installed surveillance cameras on their campuses. Those systems, aided by AI,

WITH SUPPORT FROM AT&T

THE CHRONICLE OF HIGHER EDUCATION

now have the potential to analyze much larger amounts of visual data and identify more types of threats than ever before.

The boom in new safety technology comes at a time when campus-safety offices are facing several challenges — mostly tight budgets and fewer qualified applicants for police-officer jobs. Campus-safety leaders say that while emerging digital tools cannot replace the vital role that security officers play, there aren't enough human eyes to scan an entire campus. New technology, much of it based in machine-learning principles, is already proving capable of helping campus police increase their coverage and identify threats more often and more quickly.

Instead of taking the costly step of installing entirely new platforms, most institutions are augmenting or retrofitting their existing technology to better prevent and solve campus crimes, monitor crowd behavior, and detect other threats.

Campus-safety leaders say that while emerging digital tools cannot replace the vital role that security officers play, there aren't enough human eyes to scan an entire campus.

But those new tools come with concerns about privacy. Longstanding worries about inaccuracies within AI algorithms — ones that can disproportionately and negatively affect women and underrepresented groups — and the slow rollout of facial-recognition software have created controversy within many institutions. Colleges are expanding their privacy policies — or holding off on putting new digital tools to work until they can clearly explain to campus stakeholders just how they plan to use them.

Widening (and sharpening) the lens

When it comes to securing today's campus, no technology plays a greater role than surveillance cameras. Usually located in well-traveled spaces and clearly marked with signs, cameras have become a constant presence on almost all campuses, large or small.

Cameras and the systems that operate them are ripe for upgrades that can improve campus safety, says L. Angela Webb, president of the International Association of Campus Law Enforcement Administrators, a group with 10,000 members in 30 nations.

"A lot of the energy is going into improving camera systems with enhanced AI capabilities. We can improve our monitoring of events and track distant parts of a campus in ways we never could before," adds Webb, who is also the associate vice president for campus safety at Rhodes College. "We can add analytic capabilities that give us a clearer picture of events in real time."

New "filters" that can analyze videos help college police departments determine if people are fighting or merely indulging in horseplay, or if someone is preparing to use a weapon, says Anthony Morgan, chief of public safety at Bucknell University. "We can also better monitor political protests and other mass events without an overblown police presence, which can sometimes cause tension," he adds.

Improving camera capability without replacing an entire system is important for budget-strapped institutions; each system can cost $500,000 or more. Upgrades are much more affordable, says Timothy Munro, president of the Northeast Colleges and Universities Security Association, a group with members from 70 institutions along the Atlantic coast.

"Vendors have come to realize they can make the case for software you can plug in to add to your security systems," adds Munro, also the director of campus safety at Skidmore College. "The good news is a lot of it really can enhance your capabilities."

Some colleges are looking to add airborne cameras. Bucknell is investigating whether it can afford to employ drones that "patrol" remote and wooded areas of campus by taking and relaying images to security-office video screens.

Beyond surveillance, some colleges are beginning to explore whether to buy AI-outfitted robots to handle some security jobs, such as identifying parking violators and writing tickets, Webb adds.

Detecting immediate threats

AI-aided camera systems can also be used to locate vehicles tied to crimes or individuals who may not belong on campus. Improvements in license-plate-reading products now offer institutions a strong prevention tool and an opportunity for campus police to respond immediately after a threat is identified, says Webb.

Many of the latest tools store data in the cloud and can link license-plate images with police databases that identify stolen vehicles or drivers with warrants.

At Rhodes College, cameras have been retrofitted to include heat-detection capabilities. "These help us determine whether something cameras have picked up really constitutes a threat, and especially at night, when it can be hard to get a clear picture," Webb says.

Heat-detection devices send officers an immediate alert. They are sensitive enough to capture and develop images that allow officers to determine whether a trespasser is a person, a wayward animal, or something else.

AI-infused software that counts the number of people in a particular area of a campus is also becoming more popular with campus-security officers. At Skidmore, a tool that adds up the number of cell phones within a building can alert them to early signs of trouble.

"It's a pretty reliable tool that creates a heatmap that can tell us if people are amassing at odd times or in odd places," says Munro. "It just bolts on to our wireless system. It can let us know if there's some activity, like a flash mob or something else, that we might need to monitor."

Because it doesn't collect names or cell-phone numbers, the tool protects students' privacy, he adds. (Phone-counting software also offers colleges the potential to lower some operating costs. Skidmore's facilities-management team can reduce the amount of air conditioning or heat in spaces where cell phones are not activated, since they're likely empty.)

Heat-detection devices send officers an immediate alert. They are sensitive enough to capture and develop images that allow officers to determine whether a trespasser is a person, a wayward animal, or something else.

A growing number of institutions, including Eastern Michigan University, are also investing in AI technologies that can pinpoint the presence of guns and other weapons before they are used. One in eight institutions reported using a video-based weapons-detection system in a recent survey, though nearly three-quarters say they use some kind of metal- or weapons-detection tool.

More numerous are detection tools that use sensors placed around campus to identify and locate a gun after it has been fired, says Webb. The sensors have been programmed to differentiate gunshots from other loud and sudden noises, such as car backfires or fireworks.

Improving alerts and communications

Many colleges are also putting emerging tech to work helping students and others keep themselves safe. Their goal is to avoid the delays in communications and responses that can come when people call 911 while giving people easier ways to report crime.

Undergrads at the University of Nevada at Reno recently developed an app students can use to navigate the safest route between campus buildings. The phone app informs students about the best-lit routes and notifies students in real time about hazards on campus.

At Sarah Lawrence College, safety officials will soon offer students the chance to opt into an app that will immediately identify and locate callers in need via GPS and WiFi. The goal is to "turn every cellphone into a blue-light phone," says Jim Verdicchio, director of campus safety. He adds that most campuses are likely to retain blue-light phones — which are often equipped with cameras and offer the ability to report an incident or make a request for an officer escort — because parents and students see them as oases of safety.

Though worries about privacy are keeping many colleges from implementing such tools, many safety officers see them as the wave of the future.

"Evidence shows that those cameras aren't all that useful. In fact, in 30 years of campus policing, I haven't seen even one used for an emergency. But I need to deal not just with security, but with the need to keep people feeling safe. And they love the blue-light cameras," Verdicchio adds.

New digital tools connecting campus-security offices more immediately with local and state law-enforcement agencies are also being implemented by institutions searching for ways to improve their emergency-response time and coordination abilities.

An eye for faces?

Very few campuses have considered implementing AI-powered facial-recognition software, one of the newer tools on the market, largely because of privacy concerns. Some have found less intrusive ways to use faces as biometric data — information that can determine which people are allowed access to certain parts of campus.

At Widener University's campus in Chester, Pa., officials hope to soon roll out a tool that "reads" a student or staff member's facial structure, but falls short of the precision of algorithm-based facial-recognition software. Widener plans to replace mobile ID cards for staff and students with technology scans that trace the outline of a face.

"We tried it out using our security staff here, and we've been pleased with the results," says Allison Taddei, director of campus safety at Widener. "We'd never put anything out there that we haven't tried on ourselves first. We've heard concerns about it. We'll have discussions with our community explaining why we think this is a safe and useful tool, then ask for their help in developing a policy on how we can use it."

Though worries about privacy are keeping many colleges from implementing such tools, many safety officers see them as the wave of the future.

"I'd love to add facial-recognition capabilities to our mix," says Morgan, from Bucknell. Photos of people banned from entering campus could be uploaded to an AI system, which would create an alert to

officers in the event they pop up on campus surveillance cameras.

"Otherwise, we'll be relying on little more than the human eye to find these people," Morgan adds.

Within the bounds of privacy

Federal and state regulations require colleges to maintain standards that protect students and faculty and staff members from invasions of privacy. Many governments are now tweaking those policies amid a flood of AI tools, including ones aimed at campus surveillance.

In some states, including Utah, governments are expanding policy efforts to ensure that small and rural colleges have the resources to guarantee privacy to staffers and students.

"In the next year or two, as we see more AI tools coming along, we'll also see more legislative overview and regulation," says Keith Squires, chief safety officer at the University of Utah.

To protect more personal information at public institutions across the state, Squires aided legislators and others in government as they worked to tighten policies governing the use of facial-recognition tools and license plate-reading software.

College privacy policies typically use software that blurs faces and obscures other identifying information found in images collected by campus cameras. Most institutions hold visual data, used mostly to conduct investigations and make arrests, for a maximum of 30 days before destroying them. Safety officers are typically constrained from releasing any video without the approval of a top administrator.

Colleges hoping to build trust between their departments and people on campus are becoming much more aware about the need for transparency. "We need to let people know that we don't watch videos all day, the way a casino does."

While there seems to be less concern among the younger generation about being surveilled and about privacy in general — "They don't worry about Big Brother like many of us older folks do," says Munro, from Skidmore — colleges need to continually upgrade their policies along with their technology.

Colleges hoping to build trust between their departments and people on campus are becoming much more aware about the need for transparency. "We need to let people know that we don't watch videos all day, the way a casino does," Munro says.

At the same time, safety leaders say they will continue to monitor the technology itself — and who can access and manipulate it. AI has become a double-edged sword for those charged with protecting students and staff.

"It takes a lot to stay ahead of it. We're living in a time when the bad guys can use AI to call in a false threat or mimic the voice of an administrator to trigger an alert," adds Morgan, from Bucknell. "That's what keeps me up at night."

"Campus Safety, Technology, and Privacy" was produced by Chronicle Intelligence.
Please contact CI@chronicle.com with questions or comments.

THE CHRONICLE OF HIGHER EDUCATION