The New York Times | https://nyti.ms/2MUgOdj

Could Monitoring Students on Social Media Stop the Next School Shooting?

By Aaron Leibowitz

Sept. 6, 2018

Hours after the deadly school shooting in Parkland, Fla., companies that market their services to schools began to speak up. “Governor, take pride that a Vermont-based company is helping schools identify the violence before it happens,” one company wrote on Twitter to Gov. Phil Scott of Vermont.

The chief executive of another company appeared on the news to boast of a “home run”: Its algorithms, he said, had helped prevent two student suicides.

To an anguished question that often follows school shootings — Why didn’t anyone spot the warning signs? — these companies have answered with a business model: 24/7 monitoring of student activity on social media.

Often without advance warning to students and parents, the companies flag posts like those of Auseel Yousefi, who was expelled in 2013 from his high school in Huntsville, Ala., for Twitter posts made on the last day of his junior year. “A kid has a right to be who they want outside of school,” he said later.

More than 100 public school districts and universities, faced with the prospect that the next attacker may be among their own students, have hired social media monitoring companies over the past five years, according to a review of school spending records. And each successive tragedy brings more customers: In the weeks after the Parkland attack, dozens of schools entered into such contracts, even though there is little evidence that the programs work as promised.

The customers have included districts reeling in the aftermath of shootings, like the Newtown Public Schools in Connecticut; some of the nation’s largest urban school systems, like Los Angeles and Chicago; and prominent universities like Michigan State and Florida State. The monitoring is one of a host of products and services, including active shooter insurance and facial recognition technology, that are being marketed to schools amid questions about their value.

“If it helps save one life, it’s worth every dollar spent on it,” said Chris Frydrych, the chief executive of Geo Listening, a California company whose website says, “Don’t miss out on the opportunity to listen.”

In many cases the monitoring contracts have not worked out as planned. There is little evidence the companies have helped ferret out brewing threats of violence, bullying or self-harm, according to a review of contracts, marketing materials and emails obtained through public records requests.

But in hiring them, schools expand the traditional boundaries of their responsibility, and perhaps, experts say, their liability. And, the documents show, they vacuum up hundreds of harmless posts, raising questions about student privacy.

One of the posts by Mr. Yousefi, now 22, said he was going to “chop” a teacher “in the throat,” which he said was an inside joke among the class, the teacher included. He believes his posts were brought to the school’s attention by a social media monitoring company seeking clients.

“It takes authority and extends it to an inappropriate extent in a way that’s truly terrifying,” he said. Shortly afterward, the district hired a firm to monitor posts, and more than a dozen students were expelled.

The monitoring programs have often been initiated without notifying students, parents or local school boards. Because of their relatively low cost — contracts typically range from a few thousand dollars to $40,000 per year — the deals can get buried in school board agendas.

In their advertising, the companies promise much, but when contacted, they declined to give details on specific incidents, citing nondisclosure agreements and student privacy laws. Many schools also declined to give details of instances in which they used the companies’ information.

Interviews and marketing materials help paint a picture of the companies’ basic approach. Some apply and pay for access to social media companies’ public data, such as Twitter’s so-called data fire hose, which gives users the ability to access and analyze public tweets in bulk.

Auseel Yousefi was expelled from his high school in 2013 for posting Twitter messages he insists were a joke but the school viewed as threatening. Audra Melton for The New York Times

Rather than asking schools for a list of students and social media handles, the companies typically employ a method called “geofencing” to sweep up posts within a given geographic area and use keywords to narrow the pool. Because only a small fraction of social media users share their locations, the companies use additional clues, like a user’s hometown, to determine whose content is worth flagging.

School officials are alerted to flagged posts in real time or in batches at the end of each day. Burlington High School in Massachusetts typically receives two to six alerts per day from Social Sentinel, the company based in Vermont, according to a list of alerts from 2017. Many consisted of normal teenage banter.

“Ok so all day I’ve wanted my bio grade up online and now that it’s up I’ve decided I want to die,” one Twitter post said.

“Hangnails make me want to die,” said another.

By its count, Social Sentinel has contracts in more than 30 states.

“We’re a carbon monoxide detector,” said Gary Margolis, the company’s chief executive and a former campus police chief. “If a student is posting about not liking their teacher, that’s not what we pay attention to. If a student is posting about shooting their teacher, we would hope we’d be able to find something like that.”

Mark Pompano, the security director for the school district that includes Sandy Hook Elementary in Connecticut, has vetted hundreds of school safety products since the mass shooting there. In 2015, impressed by Social Sentinel’s pitch, he gave the company a try for a few months, but it never caught anything serious, he said.

Social Sentinel struggled to weed out posts from the Twitter account of a nearby liquor store, records show.

“I cannot recall a single incident that we used Social Sentinel to pursue some type of security threat or anything like that,” Mr. Pompano said. “If something doesn’t work, we’re not going to stick with it.”

Today, Mr. Pompano said, the district relies mostly on tips from students, a system that works well if there is an atmosphere of trust. “It goes back to human intelligence, where kids have at least one trusted adult,” he said, “knowing what they’re telling them is confidential.”

In a few cases, school administrators said, monitoring services have helped them identify students who appeared to be at risk of harming themselves. More rare were instances in which an imminent threat to others was thwarted. In 2015, as the first anniversary of a shooting at Florida State approached, a post expressing sympathy for the gunman and an intent to visit the campus was intercepted by Social Sentinel, the campus police chief said. The man was stopped on campus and warned to stay away. When he returned, he was arrested.

Patrick Larkin, an assistant superintendent in Burlington, Mass., said he receives alerts on his phone in real time from Social Sentinel. “Nineteen out of 20” come from people who are not even his students, he said earlier this year.

Real threats, administrators said, are more often flagged by vigilant users, as was the case with the Parkland gunman, whose troubling comments on YouTube were reported to the F.B.I.

Mr. Larkin said Social Sentinel helps him sleep easier at night. And because it can track only public posts — nothing that requires a “friend” request — he doesn’t see it as an intrusion.

“My concern was, what if it’s some odd hour and some kid tweets something I don’t see?” he said.

Mr. Margolis said it is hard to demonstrate that harm has been averted. “How do you measure the absence of something?” he said, adding that Social Sentinel’s algorithms have improved in recent months.

One client, Michael Sander, the superintendent of Franklin City Schools in Ohio, said he had planned to contact the police about a Twitter message that read, “There’s three seasons: summer, construction season and school shooting season.” But the poster appeared to attend school in Franklin, Wis. — not Ohio.

Some companies have backed off from early promises, including creating watch lists that tracked specific people. LifeRaft, based in Nova Scotia, told the Salem-Keizer Public Schools in Oregon that it could help the district find “behavioral information” on “individuals of concern.” The company also vowed to monitor the conversations of “groups and networks” connected with those individuals.

Mr. Margolis of Social Sentinel said it was difficult to demonstrate that harm had been averted. “How do you measure the absence of something?” he said. Hilary Swift for The New York Times

Mary Jane Leslie, the vice president of LifeRaft, acknowledged that the language was “creepy,” saying, “To be frank, I don’t think the software ever really did that.”

She added that the company no longer markets its services to schools.

To use social media data, monitoring companies must agree to specific rules, which were tightened after multiple companies were condemned by the American Civil Liberties Union in 2016 for helping police clients surveil activists in the Black Lives Matter movement. Twitter, Facebook and Instagram cut off the firms’ data access. Some, like Social Sentinel, dropped their police contracts to concentrate on serving schools.

The A.C.L.U. called out Media Sonar, an Ontario firm that recommended that its police clients monitor hashtags like #BlackLivesMatter, #DontShoot and #ImUnarmed. In late 2015, around the one-year anniversary of the death of Michael Brown in an encounter with the police in Ferguson, Mo., Media Sonar briefly contracted with the Ferguson-Florissant School District, which asked for alerts on the terms “protest” and “walkout.”

Kevin Hampton, a spokesman for the district, said the service was used strictly for safety purposes. Media Sonar did not respond to interview requests.

But privacy advocates questioned whether safety was the companies’ only motive. “The companies seem to dance back and forth” between marketing themselves for public health and student discipline, said Kade Crockford, director of the A.C.L.U. of Massachusetts’ Technology for Liberty program. “Those two goals seem fairly at odds and somewhat contradictory.”

In 2013, the Huntsville City Schools in Alabama enlisted a consulting firm for a surveillance program that led to the expulsion of 14 students, 12 of them African-American.

Casey Wardynski, the district’s former superintendent, told local news organizations that the program had helped break up a local gang, and some students were expelled for wielding guns on Facebook.

One student had been accused of “holding too much money” in photographs, an investigation by the Southern Poverty Law Center found, and one was suspended for an Instagram post in which she wore a sweatshirt with an airbrushed image of her father, a murder victim. School officials said the sweatshirt’s colors and the student’s hand symbol were evidence of gang ties, according to the investigation.

Monitoring students’ lives off campus is untested terrain. School lawyers are advising administrators to be “very cautious,” said Sonja Trainor, the managing director of legal advocacy for the National School Boards Association. Districts “tend to find that they’re inundated with information, and it becomes very difficult to establish parameters for issuing warnings to the community,” she said.

In 2013, the Glendale Unified School District in California hired the company Geo Listening in response to student suicides in which online bullying had been cited as a factor.

Lilly Leif, a 2017 graduate of Glendale’s Crescenta Valley High School, said she was summoned to the assistant principal’s office after using an expletive in a post about her biology class. The assistant principal showed her a printed copy and asked her to change her account settings to private, she said.

“She said it reflected poorly on my high school and my teacher,” said Ms. Leif, 19, now a college sophomore.

In another instance, Ms. Leif said, an administrator asked students to delete a message promoting a school fund-raiser at “Blaze Pizza” and “Baked Bear” — actual pizza and ice cream establishments — because of the apparent allusions to marijuana.

Rene Valdes, the district’s former director of student support services, said the program included teaching students online etiquette. “The conversation with the kid would be, ‘Realize that companies are now monitoring social media before they hire people,’” Mr. Valdes said.

After an outcry in Glendale, the State Legislature passed a 2014 law requiring California schools to notify students and parents if they are even considering a monitoring program. The law also lets students see any information collected about them and tells schools to destroy all data on students once they turn 18 or leave the district.

That’s no longer a concern for Glendale, which dropped its contract with Geo Listening last year.

“We discovered more and more kids were using Instagram and Snapchat, and those were not being monitored by Geo Listening,” Mr. Valdes said. “It seems like the kids are always two steps ahead of the adults.”

A version of this article appears in print on Sept. 6, 2018, Section A, Page 1 of the New York edition with the headline: Online Eyes For Watching Students 24/7