The New York Times

How Much School Surveillance Is Too Much?

Florida's proposed database will test the limits.

By Charlie Warzel
Mr. Warzel is an Opinion writer at large.

Published Aug. 27, 2019 Updated Aug. 28, 2019, 11:47 a.m. ET

Back-to-school season is upon us and the future of child surveillance may soon be underway in Florida.

Last month I referenced a proposed school surveillance program in the state, where lawmakers were planning to introduce a statewide database "that would combine individuals' educational, criminal-justice and social-service records with their social media data, then share it all with law enforcement."

This month we know a bit more about what that program will look like, thanks to a 19-slide PowerPoint presentation released by the Florida Department of Education. Turns out, it's quite extensive. You can look at the full presentation here and read a local news article on the report here.

A few highlights:

Officials are calling it a "safety portal" because the software will pull information from multiple databases, rather than host it all itself. Much of the information inside will be pulled from platforms like Twitter, Facebook, Instagram, YouTube, Reddit, Flickr, Google+ and Pinterest. Software deployed by the state will scan social media and general websites. It will monitor and store students' social media posts as well as the geolocation, showing where the posts were made.

According to the PowerPoint, the software will monitor keywords on five topics: "gun," "bomb," "bullying," "mental health" and "general," which is vague enough to leave room for virtually any topic. Recorded information will go into the state database (portal) and school districts, and specific "Threat Assessment Teams" will get alerts if it's determined there's a threat.

In the age of mass school shootings, such a program may seem comforting to some parents. But the program's sweeping collection parameters and the combination of information from multiple state databases mean that the portal will ultimately be home to a great deal of sensitive information. And the portal remains an excellent example of how programs designed to protect may have serious unintended privacy consequences.

For instance, according to the PowerPoint, the portal will not "store information about students' race, religion, disability or sexual orientation." However, information in the portal will contain School Environmental Safety Incident Reporting tags, which could reveal information about students who were

bullied because of race, sexual orientation or disability. This type of de-anonymizing, even if accidental, is common when cross-referencing different databases.

For whatever safety it could add, automating systems to catch school shooters and other threats also increases the likelihood of technical errors. One slide from the PowerPoint notes that the portal will assess potential threats and monitored social media posts using "programmatical scoring that can help in determining relevancy of each returned record."

The slide is vague on what exactly "relevancy" means in this case, and without algorithm transparency, it's unclear whether the scoring system will bias students who may be vulnerable because of, say, a disclosed mental health issue. And since relevancy is left vague, it's unclear how often a threat will trigger the portal's flagging mechanisms. Depending on algorithmic calibration, teams could be inundated with false alarms or, perhaps, not receive them at all.

But as with any database, the biggest concern is who will have access to the data of hundreds of thousands of students. Here's how Amelia Vance, who directs the Future of Privacy Forum's Education Privacy Project, put it in an email:

> There are over 4,000 schools in Florida; if we assume each school has a three-person minimum threat assessment team, that equals over 12,000 people who will have access to this portal. Even if Threat Assessment Teams are only at the district level, that is a minimum of 200 people for the 67 districts. With that many people able to access the system, it is highly likely that there will be multiple security vulnerabilities."

Perhaps the system works flawlessly (though I'm quite skeptical). Early reports suggest that the database may have serious limitations. Still, it's hard not to think about the impact on the students themselves. The surveillance state seems to be encroaching on every aspect of minors' lives lately. It comes from all angles — from overeager parents, facial recognition in summer camps and, increasingly, in school.

And it shows no signs of letting up. Near the end of the PowerPoint presentation is a slide that says, "What's Next?," which includes an action item on collecting School Environmental Safety Incident Reporting data (including categories from arson to tobacco use).

"It is currently collected 3 times a year," the slide reads. "A weekly collection is being considered."

From the Archives: "The Candid Picture"

As we continue to have the facial recognition debate, this piece from 1950 by Jacob Deschin is a great read:

> The camera is, inescapably, an intimate instrument. It records for a fraction of a second a fellow being as he is. The man who operates it for public dissemination then, must have a deep sense of respect for all human life. I detest and always have detested the sneak snapshot. The photograph should never be used as a sort of modern revival of medieval bear-baiting or a Roman holiday designed to bring amusement to the masses at the expense of depreciating any human being.

Deschin would not have liked the iPhone.