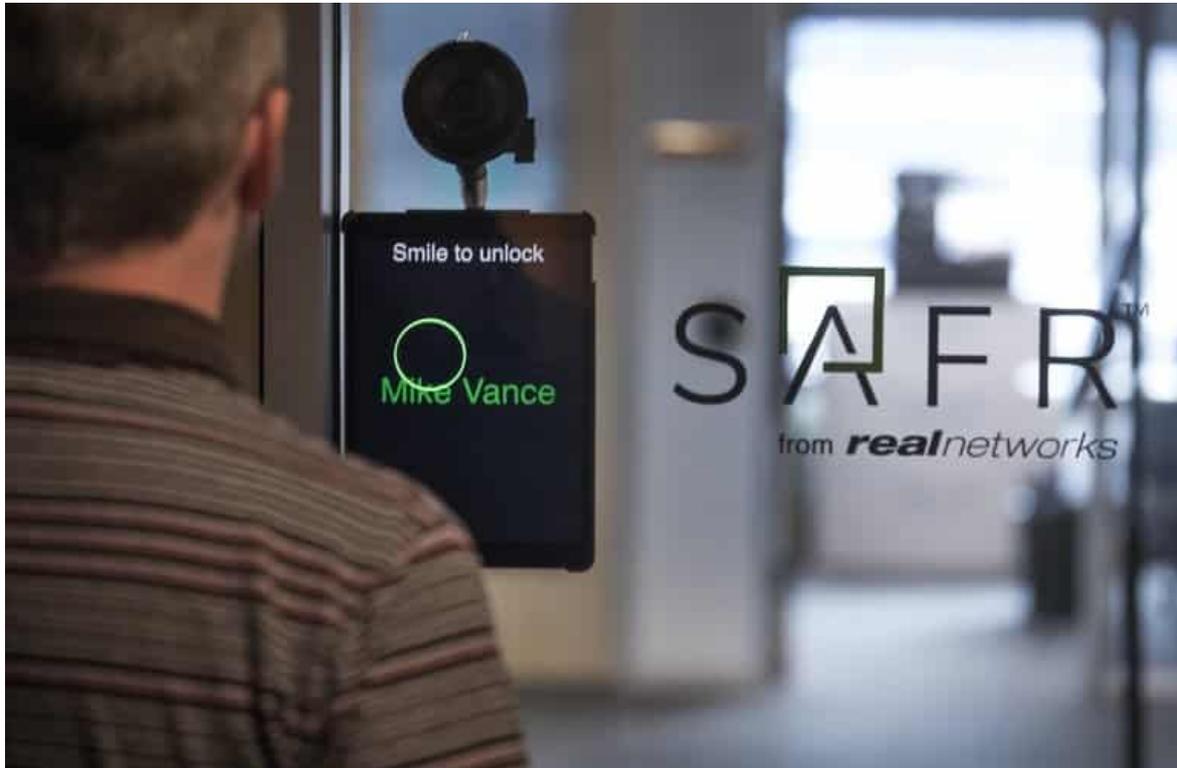


Should Facial Recognition Systems Be Installed In U.S. Schools?



Parents are protesting less than they should biometric identification for their children will be absolute before they even graduate from high-school. Technocrats generally steam-roller over ethical and Constitutional concerns, pleading efficiency and convenience. □ TN Editor

RealNetworks is offering schools a new, free security tool: facial-recognition software. But as the technology moves further into public spaces, it's raising privacy concerns and calls for regulation — even from the technology companies that are inventing the biometric software.

As Mike Vance approaches the glass door that leads to RealNetworks' engineering office, he smiles slightly at a small camera mounted in front of him. Click. The door unlocks, responding to a command from software powering the camera that recognized Vance's face and confirmed his identity.

Vance, a senior director of product management at the Seattle tech company, leads the team that created Secure, Accurate Facial Recognition — or SAFR, pronounced “safer” — a technology that the company began offering free to K-12 schools this summer.

It took three years, 8 million faces and more than 8 billion data points to develop the technology, which can identify a face with near perfect accuracy. The short-term goal, RealNetworks executives say, is increased school safety.

“There’s a lot of benefit for schools understanding who’s coming and going,” Vance said.

The software is already in use at one Seattle school, and RealNetworks is in talks to expand it to several others across the country. Looking ahead, RealNetworks — known for video- and music-streaming software introduced in the early 2000s — plans to sell SAFR to various industries, though the company is staying completely mum on the details for now.

The introduction of the technology has thrust RealNetworks into the center of a field that is growing quickly as software gets better at identifying faces. But growing along with it are privacy concerns and rising calls for regulation — even from the technology companies that are inventing the biometric software.

Facial-recognition technology is already common, used in everything from photo apps that sort pictures of people, to unlocking an iPhone, to law-enforcement agencies searching databases of driver’s license photos.

Facial recognition is used, broadly, in two ways, said Oren Etzioni, CEO of Seattle’s Allen Institute for Artificial Intelligence, the sister organization to Paul Allen’s brain science institute. One is consumer convenience, such as grouping photos, and the other is for surveillance and tracking.

The big tech players have been involved for years: Microsoft markets Face API for companies to identify and group similar faces for apps and other products, while Amazon has Rekognition, which came under fire

earlier this year when the ACLU asked the company to stop selling it to law-enforcement agencies. Google, Apple and Facebook are also in the game, as tagging and grouping photos on smartphones illustrate.

But now, as RealNetworks' SAFR shows, the technology has been moving further into public spaces. And with that, privacy advocates wonder if people fully realize how often their faces are being scanned, and advocates and the industry alike question where the line is between the benefits to the public and the cost to privacy.

Learning a face

Facial-recognition technology functions much like fingerprinting — each face has its own unique signature, and companies teach machines to recognize and match people's unique features.

RealNetworks' technology maps 1,600 data points on each face it sees. The team has been "training" its machine for about two years, since the launch of RealTimes, its free app that lets people build photo slideshows. Baked into the 3,300-word user agreement for that app is language that allows RealNetworks to use customer photos to train its facial-recognition system.

SAFR doesn't know the identity of people in the RealTimes photos, Vance said — there are no names, addresses or other identifying information in the massive database of 8 million faces. But what it can do is tell if two faces are the same person. It's gotten so accurate that it can tell identical twins apart and match family photos of the same person even if they were taken decades apart.

SAFR relies on being able to identify people "in the wild," or acting candidly, not posing.

"The great things about those kinds of faces is that they're people doing things that they naturally do in life," Vance said. "They're not mug shots or canned shots. You can overtrain a system for people looking squarely into the camera. But when you're walking around here, when you're walking around a school, you're not always looking squarely at the camera."

Many face-recognition technologies can also identify basic demographics of a person. Microsoft's Face API, for instance, can guess your age with just one photo — a feature that has gotten more accurate since it was first released in 2015 to middling user reviews.

That has led to concerns of bias, though, especially since a study at MIT's Media Lab found some big tech companies' facial-recognition apps had error rates up to 35 percent higher when identifying women with darker skin compared to men with lighter skin. Some feared that could lead to misidentifying women and people of color, a troubling issue especially if the systems are used by law enforcement.

Microsoft has acknowledged the bias issues and is taking steps to better identify diverse faces, broadening the database it uses to train its system by adding photos of more diverse people.

RealNetworks, however, hasn't trained its software to identify someone based on race. You couldn't, for example, ask SAFR to alert you when a white man walks in a door because it won't know which faces are white.

[Read full story here...](#)