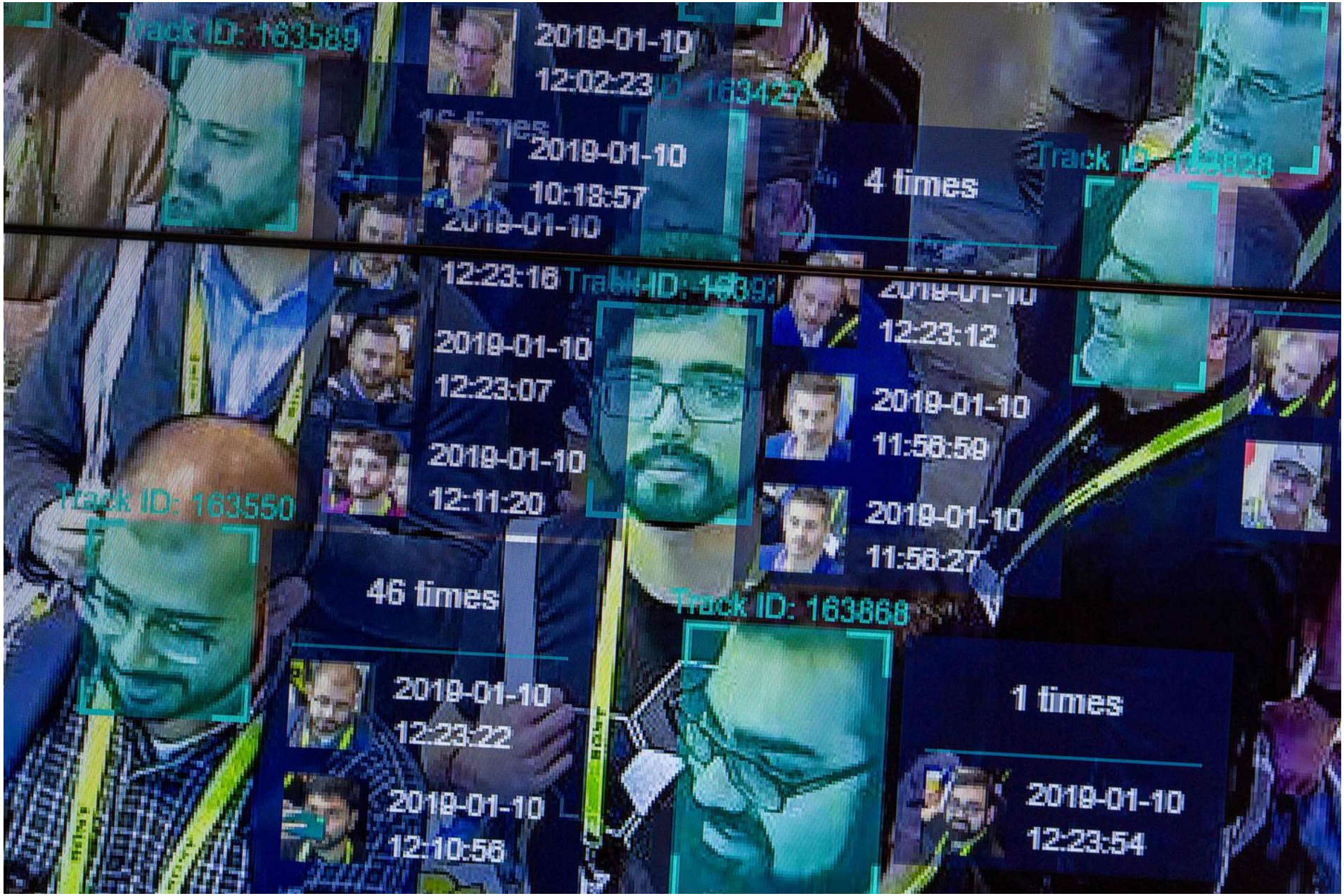
Somerville moves to ban facial recognition surveillance

By Andy Rosen Globe Staff, May 10, 2019, 8:45 p.m.



A demonstration using artificial intelligence and facial recognition in dense crowd spatial-temporal technology was held earlier this year at the CES trade show in Las Vegas. DAVID MCNEW/AFP/GETTY IMAGES/FILE/AFP/GETTY IMAGES

Somerville officials have proposed a ban on the use of facial recognition in police investigations and municipal surveillance programs, part of a growing backlash against a rapidly evolving technology that critics fear may lead to false identifications and bias against minorities.

A bill to ban the technology was introduced at the Somerville City Council Thursday, and appears headed for passage later this year. Meanwhile, the state Legislature is considering bills that would enact similar prohibitions statewide. And across the country, cities such as San Francisco and Oakland are moving quickly to ban facial recognition in municipal uses.

In Somerville, the proposed ban already has the backing of nine of 11 city councilors, as well as Mayor Joseph Curtatone. The American Civil Liberties Union, which supports such crackdowns, says Somerville is the first East Coast city to push for a ban.

The lead sponsor of the Somerville measure, Councilor Ben Ewen-Campen, said he could see facial recognition being useful in serious emergencies, such as terrorism cases. But he doesn't think the technology is ready, nor has the public considered its full implications.

"I think large numbers of the public may eventually be convinced that there is a useful need for this kind of thing," he said. "But to use cases like that as the thin edge of a wedge to allow the government to just, in real time, surveil every person in every public space in our community, I think that's where the real danger is."

Ewen-Campen said he does not know of any ongoing surveillance programs in Somerville that would be banned by the measure, but said it is important to discuss the technology before it gets into widespread use.

And Curtatone, too, said he is concerned that “the ease and efficiency of tech can also be so vast and so broad that it can infringe on our right to privacy.”

At the state level, similar bills have attracted a significant base of support. One measure, proposed by Senate majority leader Cynthia Stone Creem, also has the support of minority leader Bruce E. Tarr.

That bill would place a moratorium on the state government’s use of face recognition and other “remote biometric surveillance systems” until the state has developed a framework for who can collect such information, how the data will be managed, how it will be audited, and what subjects’ rights will be.

“I don’t think we’re arguing that this is something that would never work,” Creem said. “I just would argue that at this point . . . it’s pretty clear that it’s not developed.”

Just as facial recognition technology can help social networking services such as Facebook to identify friends in your uploaded pictures, it can also help police and other government agencies look for possible suspects and potential threats in images collected by investigators or taken by the thousands of public cameras in use.

But civil rights advocates say that there are not nearly enough safeguards in place to make sure that the technology is being used ethically, or even whether it works correctly.

For instance, research published by the Massachusetts Institute of Technology and Stanford University last year found that commercial facial recognition programs misidentified the gender of dark-skinned women as much as one-third of the time, while they made similar errors on light-skinned men in fewer than 1 percent of cases.

Moreover, alarm over potential misuses of the technology by governments has grown with the disclosures that the Chinese government had used facial recognition as part of its crackdown on the Uighur ethnic minority. The New York Times reported in April that law enforcement in one Chinese city ran 500,000 scans in a single month over surveillance cameras to identify Uighurs.

Kade Crockford, who runs the Technology for Liberty Program at the ACLU of Massachusetts, said facial recognition should not be used by law enforcement because it is unreliable and the public has not had enough time to consider the implications of its use.

Facial recognition systems are used by some US police departments; Amazon, for example, has been pressured by people in the artificial intelligence field to stop selling its facial recognition system to law enforcement agencies.

Plymouth's Police Department was recently pitched on a facial recognition technology by a Cambridge startup that sells surveillance tools to law enforcement. Suspect Technologies cofounder Jacob Sniff had proposed that Plymouth police install cameras with facial recognition capabilities in public buildings around town, and suggested the department could tap into a statewide database of driver's license photos, according to e-mails the ACLU obtained through public records requests.

However, the company was told the state had denied previous requests to access the photo database. And Plymouth police Chief Michael E. Botieri told the Globe in a phone interview in April the town won't use the Suspect Technologies program as proposed. Instead, Plymouth will test out the company's software — on a free-trial basis — in criminal investigations to compare faces in video evidence against those in the department's booking photos.

The software, Botieri said, is simply "an investigative tool," and even if it registers a match, "you wouldn't just arrest someone based on what the computer says. It just points you in a direction to investigate."

"I totally get the privacy issue," Botieri added. "It's something people feel is intrusive."

In a statement to the Globe Friday, Sniff said his company "strives to provide video analytical solutions that enable public safety authorities to solve crime, improve the quality of life for their local communities, and provide technology that is designed to respect privacy and protect the innocent."

Facial recognition is but one of several new technologies that have extended the surveillance reach of law enforcement, and have raised a host of new privacy questions that governments around the United States are racing to resolve. In Massachusetts, the State Police ran a program for more than three years collecting license plate data of every vehicle that crossed the two Cape Cod bridges — more than 100 million trips — without disclosing its use to drivers.

Ewen-Campen, the Somerville councilor, is pushing another measure that would increase public oversight of surveillance technology in Somerville. But facial recognition, he added, is in a class of its own, "and that's why until we have that conversation about what the regulations are, what the guardrails are, a ban is really the only way that we can go."

Matt Rocheleau and Christina Prignano of the Globe staff contributed to this report. Andy Rosen can be reached at andrew.rosen@globe.com.