

## Polls shows Utahns aren't concerned about facial recognition software. Lawmakers and privacy advocates say they should be.

Salt Lake Tribune

February 13, 2020

By Paighthen Harkins

<https://www.sltrib.com/news/2020/02/13/polls-shows-utahns-arent/>

Many Utah lawmakers were alarmed last year when they learned that federal law enforcement had used facial recognition technology to scan thousands of photos in the state's driver license database for suspects.

Legislators [peppered Department of Public Safety Commissioner Jess Anderson](#) with questions in a [September meeting](#), as [a researcher claimed](#) that "nearly every Utah adult has been affected by facial recognition technology." They debated an [initial bill](#) on the issue in November and now are considering a new bill from Sen. Kirk Cullimore, R-Draper.

Despite the uproar, most Utah residents say they approve of law enforcement searching the state database for suspects, according to a recent statewide poll by The Salt Lake Tribune and Suffolk University.

Just over 63% of Utahns polled said they either somewhat approve or strongly approve of law enforcement using the technology to comb the state's driver license database. Just over 29% disapproved and 7.6% said they didn't know.

Pollsters surveyed 500 Utahns from Jan. 18 to Jan. 22 over landlines and cellphones. The poll's margin of error is plus or minus 4.4 percentage points.

Two Utahns who support law enforcement use of the technology told The Tribune that they weren't worried about police looking at their faces because they haven't done anything illegal. "I know there's reservations, that people are worried that it's invasive, that it kind of interferes with people's rights, and I can understand that," said Katie Stack from Ivins, "but at the same time, for me, if you're not doing anything wrong, why be worried about it?"

Stack, 31, added a caveat to her approval: Facial recognition technology shouldn't be the end-all, be-all for identifying suspects. It should just be "one piece of the puzzle," she said.

Darren Day, of North Salt Lake, said he sees the driver license database as just another part of society ripe for data-mining in an increasingly technological world. If one chooses to opt in by getting a license or posting on social media, he said, they also opt in to the consequences of that choice.

"We all know that stuff stays out there," the 46-year-old said. "If we're doing improper things, we're gonna be held accountable."



ACLU Utah and the libertarian Libertas Institute have both spoken out against use of facial recognition technology in Utah. Connor Boyack, president of the institute, told The Tribune he wasn't surprised by the poll's findings — and that they don't change how lawmakers should feel about the practice.

"You might find similar numbers, or even greater numbers, of people who are supportive of government access to our emails, to our phone calls, to our computers," he said. "Just because there appears to be many people who are fine with government surveillance does not mean that the government should have unfettered access to surveil people."

Gay Anthony, 66, agreed with Boyack. The Taylorsville resident said she disapproved of law enforcement looking through the database with facial recognition technology for the same reason she doesn't like how social media sites somehow know what products she's interested in purchasing.

"I'll be talking to my best friend about something, and then it's on our Facebook Apps," Anthony said. "You know, if we're talking about going on a cruise or something and then we get advertisements for cruises."

It's weird, she said, and an invasion of her privacy.

But privacy isn't the only concern when it comes to facial recognition technology.

It can also incorrectly identify possible suspects in cases because it sometimes can't accurately discern between different people of color, women and older and younger people, said Marina Lowe, ACLU Utah's legislative and policy counsel. Anderson acknowledged some of those points during the September meeting.

In a worst case scenario, Boyack said, the technology could send a SWAT team to someone's door based on a partial and incorrect facial match and that person could be accidentally shot.

"Is that likely to happen? No," he said. "Is it within the realm of possibility? Sure."

When the technology is being used in connection with potential criminal liability for someone, Lowe said, there should be a high level of certainty that it's pointing out the right person.

"The point is that people should have a say in whether their face is going to be searched by law enforcement," Lowe said, "especially when they signed up for their face to be captured by the government for an entirely different purpose."

Utah lawmakers began discussing how to regulate the use of the technology after the Washington Post and New York Times last year reported that the FBI and Immigration and Customs Enforcement mined driver license databases in many states, including Utah, analyzing millions of motorists' photos without their knowledge.

Since then, a facial recognition technology startup, Clearview AI, has made headlines nationally for scraping photos from social media sites for its own database. Its technology, marketed only to law enforcement agencies, allows investigators to upload, for instance, images from surveillance footage to search for a match.

The New York Times [reported last month](#) that the tool "could end your ability to walk down the street anonymously."

The Utah attorney general's office met with Clearview AI to discuss the technology, spokesman Richard Piatt said, but decided not to use it because "it has not been properly vetted."

Department of Public Safety spokeswoman Marissa Cote said DPS isn't using the technology and doesn't know of any law enforcement agencies in Utah that are.

To find consensus on rules and protections for using facial recognition technology, Cullimore has been working with groups, including the ACLU, Libertas Institute and the Department of Public Safety. He told The Tribune he's not sure what those requirements will be just yet, but he hopes to get a bill passed this session.

The legislation, Cullimore said, will likely go further than [Sen. Daniel Thatcher's November proposal](#), which added a disclaimer when a person applies for a license or government ID that warns the photos would be entered into a database that law enforcement could search it using facial recognition technology. It also codified the existing practice that recognizes DPS is the only state entity authorized to use facial recognition technology.

Cullimore said he hopes the bill will also address the future uses of this technology, such as for live streaming, where law enforcement could conceivably search a crowd for faces in real time. "Anytime that government can breach what could be deemed as privacy, we need to at least be cautious about it and see that there's not violations of constitutional rights — or that there could be the perception of that," he said.

For instance, he asked, if police could search live footage of a protest for faces, could that stymie free speech and assembly? Might people be less likely to show up for fear of being surveilled?

Cullimore said he's had discussions about adding an opt-in or opt-out feature in the driver's license application process. Some have suggested the legislation should require a warrant for these kind of searches. Cullimore said he's skeptical of both those options.

"But," he conceded, "I guess I'm pretty open right now. I am a little bit hesitant to have these databases used for any and every purpose under the sun, but I recognize that there are legitimate purposes. And so, again, let's find out where that happy median is."