After Stops and Starts, Utah Enacts Biometric Guardrails

Unchecked surveillance concerns forced the state's public safety agency to re-evaluate how it uses biometric technology with a focus on a more transparent, audit-ready process, bolstered by implicit bias training.

BY LUCAS ROPEK

OCTOBER 5, 2020

https://www.govtech.com/policy/After-Stops-and-Starts-Utah-Enacts-Biometric-Guardrails.html

New policing technologies routinely solve crimes that would've been deemed unsolvable a mere decade ago. Yet while these technologies supply law enforcement with startling new powers, governments often find themselves lacking the regulatory frameworks to guide how the tools can and should be used.

One such example of this is Utah, where a recent legislative attempt to regulate facial recognition use collapsed earlier this year. The Department of Public Safety (DPS) recently announced internal regulations designed to curb abuses and overreach, but critics say these don't go far enough to protect civil liberties.

Last year, researchers at Georgetown University's Center on Privacy and Technology published a report showing how agencies in multiple states, including Utah, had been sharing driver's license data with federal law enforcement, including the FBI and Immigration and Customs Enforcement (ICE).

The report inspired a torrent of bad press, as well as questions from state legislators about the extent of the program and why officials had not been adequately informed. How widespread was the program and had it been used to target undocumented immigrants?

During a Law Enforcement and Criminal Justice Interim Committee meeting in September, DPS Chief Brian Redd shot down the idea that federal agencies like ICE had unmitigated access to their database or that the data sharing was used for deportation operations.

"We were conducting checks not for immigration and customs enforcement removal operations (ERO), but for homeland security investigations for criminal investigative purposes," said Redd.

Utah's Statewide Information and Analysis Center (a fusion center nested within DPS) has operated the facial recognition system since 2010, routinely mining data from millions of IDs within the Utah DMV archive, according to researchers. State officials use the tool for their own investigations and share data with federal agencies and other parties upon request.

If a federal agency, for instance, was trying to identify an individual in a picture, they might submit it to Utah's SIAC, which could use its facial recognition program to scan accessible databases (including, frequently, the DMV), cross-checking millions of photos in pursuit of a match.

These operations have a process but critics have argued that, in the past, it didn't include enough checks and balances, nor did it operate with the proper level of transparency. In addition to the lack of a regulatory framework for how the state was allowed to use the tool, most Utahns had no idea that the program even existed.

"I think the very reaction to the story when it broke proves the point that people had no idea that this was happening," said Marina Lowe, legal and policy counsel for the Utah ACLU. "There was a real sense of outrage that there had not been any sort of legislative authority to engage in this practice."

Following its public outing, rights groups like ACLU and the libertarian privacy organization Libertas Institute lobbied DPS to shift its policies. Working together with agency officials and legislators, the groups sought to craft a state law governing the surveillance tool's usage, but like so many attempts at regulation, it ran into stakeholder disagreement that muddied the waters.

Senate Bill 218 would have regulated how facial recognition was used by Utah, restricting use to the DPS and ensuring that it was only used in cases where violent or serious crimes, like felonies or murder, were involved. It also would've barred usage in cases involving civil immigrations violations.

That legislation never got off the ground, however.

As an alternative, DPS announced its implementation of new internal protocols, designed to inject more accountability into the process. The new policies include a more auditable, policy-driven procedure for responding to outside data requests, and will also require DPS staff who operate the system to undergo mandatory implicit bias training, said Redd.

The agency continues to use its biometric system to help investigate pretty much every kind of criminal activity imaginable, Redd said.

Used an average of 40 times per month, the system assists state investigators as they pursue everything from serious crimes like sexual assault, rape and murder to relatively minor crimes like probation violations, obstruction of justice, threats and criminal mischief. It has also been used in missing persons and larceny investigations, he said.

For many who support the program, it is seen as a cost-effective and efficient tool, and criticisms of it lack context and are overblown. Sen. Daniel Thatcher, R-District 12, told *Government Technology* that, in many cases, the program is purely a fraud mitigation tool, something to stop people from exploiting the state's driver's ID system.

Yet critics like Lowe push back on the idea that just because you have a driver's license, you've somehow signed up for inspection by myriad police agencies.

"People take a driver's license picture for the purpose of being able to use an automobile on the roads," said Lowe. When you enter into that contract with the DMV, however, there is little understanding that the photo may be "placed in a database that could be regularly searched by law enforcement agencies — not just here in Utah, but by national agencies or other agencies across the United States," she said.

Facial recognition has certainly proven one of the most controversial technologies to be leveraged by state and local governments — an issue exacerbated by this year's calls for national police reform.

"As a society, Americans have consistently rejected the idea of a national biometric ID system," said

Claire Garvie, one of the Georgetown researchers that helped publish the Utah revelations last year. "Nixon called biometrics the 'mark of the devil.' Clinton said it was 'too big brotherish.' [There is] lots of skepticism around it."

Governments should seek to be more transparent about how they are using these technologies, Garvie said, because a lot of distrust emerges from the secrecy by which agencies collect and share data. Just how extensive biometric data collection is via state and federal agencies is, in many cases, still not totally clear.

"There's just a lot that we still don't know," she said.