Suresh Venkatasubramanian: Utah should opt out of the surveillance state

By Suresh Venkatasubramanian
Special to The Tribune
September 8, 2019
https://www.sltrib.com/opinion/commentary/2019/09/08/suresh-venkatasubramanian/

(Vincent Yu | AP file photo) A protester uses an umbrella to block a surveillance camera during a demonstration at the Airport in Hong Kong,

A revolution is happening in government surveillance, and we are a part of it whether we like it or not.

This growth of new and invasive technology includes body scanners at airports, facial recognition cameras, and artificial intelligence software that links it all together. Despite Utah's reverence for privacy, our state is not exempt from this trend.

In May, we learned that Utah's attorney general signed an agreement with a company to promote testing of 3D body-scanners at Utah sporting events, schools and public events. Then, in July, The Washington Post reported how Utah's Department of Public Safety scanned every Utah driver's license photo thousands of times between 2015 and 2017 with facial recognition software at the request of the FBI, ICE and police agencies. If you hold a Utah driver's license, your face has been scrutinized — without a warrant — by computer algorithms seeking to match your photo to potential suspects.

Finally, in August, the Utah Legislature debated a $2 million funding request to build a statewide surveillance system that sweeps up real-time data from social media posts, traffic cameras and 911 calls to allow an artificial intelligence "engine" to predict where criminal activity is occurring. The Rocky Mountain elk might be Utah's official mammal, but Utahns are guinea pigs to this growing demand for secret surveillance.

Law enforcement agencies often claim these new technologies are more accurate and less intrusive than prior methods. But independent test results reveal these products regularly overpromise and underdeliver. The oldest and most commonplace of these systems, the airport body-scanners, routinely fail to function accurately for people who aren't white and male. And even the most advanced facial recognition algorithms are rife with systematic errors against minority populations.

A recent test of Amazon's facial recognition technology wrongly matched photos of 28 members of Congress to mugshots of people who had been previously arrested, falsely tagging people of color at higher rates. Earlier this year, body-camera maker Axon rejected adding facial

recognition features, citing “evidence of unequal and unreliable performance across races, ethnicities, genders and other identity groups." Closer to home, Liberty Defense, the Georgia-based company seeking to test 3D body-scanners on unsuspecting Utahns, can’t guarantee their system will be effective at detecting security violations.

While companies can chip away at the technological limits, the legal challenges are more difficult. Any database of collected images can be used beyond its intended purpose. For example, when you got a Utah driver’s license photo, did you know it would be dumped into a database and scanned thousands of times by law enforcement agencies? Likewise, Liberty Defense claims their body-scanners are “less intrusive” because they search crowds of people for threatening objects, rather than tracking identities. But, unlike noticeable airport checkpoints, their scanners are designed to be hidden in public places, allowing, as Utah Attorney General Sean Reyes stated, “to potentially push the perimeter out further.”

This open-jaw approach to surveillance should not only alarm the 260,000 Utahns with concealed firearm permits, but also anyone with a wearable or implanted medical device, because most scanners can’t distinguish between a gun and a colostomy bag or an insulin pump. Finally, computerized scanners often save the resulting images, opening the door to data breaches and hacking. Earlier this year, 100,000 images of faces and license plates of people crossing the U.S. border were stolen from a federal contractor.

We need to acknowledge that increased surveillance doesn’t automatically bring increased security. Governments often pursue technologies that make people feel more secure without actually doing anything to improve overall safety, a phenomenon that privacy specialist Bruce Schneier calls “security theater.”

As governments continue to push for new and invasive surveillance technologies, we need a serious discussion in Utah about security, due process and privacy rights. When state and local police departments propose security systems with powerful scanners linked to artificial intelligence, let’s make sure the process is transparent, that privacy is protected, and that the shiny new technology actually works.

Suresh Venkatasubramanian is a professor at the University of Utah’s School of Computing and a board member of the ACLU of Utah.