Gehrke: Utah's sweeping, unreliable searches of our driver license photos need to stop
By Robert Gehrke
Published: July 15
https://www.sltrib.com/news/2019/07/15/gehrke-utahs-sweeping/

Back in October 2017, federal immigration agents sent a request to Utah law enforcement to compare a photo of a criminal suspect against about 5 million images in the state's driver license database — including, assuming you have or have ever had a Utah license, yours.
The search came back empty. Three minutes later, they did another search. Then they did another 33 minutes after that. And over the following 18 minutes did six more. Not one of them produced a match.
According to state logs provided to the Georgetown Center on Privacy and Technology, these were among hundreds of searches U.S. Immigration and Customs Enforcement requested in a two-and-a-half year span in Utah and they are part of literally thousands conducted for law enforcement at the federal level or in other states.
In fact, whether you know it or not, police in Utah scan your face and compare it to a criminal suspect nearly three times every single day.
Now, Utah officials dispute their own figures and say ICE's use of the database was much more limited.
The point remains: When we sat in that chair and had a state employee snap the worst picture any of us will ever have taken, did we knowingly sign up to be part of a massive data trove leveraged to make life easier for law enforcement?
I remember checking the box letting them take my kidney after I'm gone, but not the one letting them give my face to the FBI while I'm still using it.
As Clare Garvie, the Georgetown researcher who uncovered the data from Utah and other states, told a U.S. House committee in May, Americans have repeatedly rejected the creation of national databases. In 1981, President Ronald Reagan called it the "Mark of the Beast," President Bill Clinton later suggested it smacked of "Big Brother," and Utah was at the forefront of states opposing the REAL ID program, a nationally standardized ID card. (The state has since complied with the federal mandates.)
Now, however, a national database is essentially what we have — or perhaps a slew of national databases, is more accurate. Law enforcement anywhere in the country can simply open a case file and request a search of the faces in driver license databases and, in Utah's case, do it without a warrant or without even demonstrating necessity or probable cause.
It was a rarity, according to the state's logs, for a search to produce a match. And even when it did, studies have shown that facial recognition is often unreliable and produces the highest number of false hits among minority groups.
The searches, particularly those conducted on behalf of federal immigration officials, also undermine trust in Utah's driving privilege program, designed to allow undocumented immigrants a way to drive legally and obtain insurance.

And now that you're in the database, there's really no way out. Even if you give up your license, the database stores all past information in perpetuity — that's why there are so many more records than licensed drivers — and there is no way to opt out of the facial searches.

Some might be saying: “Relax, hippie. The driver license division wouldn’t share data inappropriately, right?”

Wrong.

In January, Utah State Auditor John Dougall issued a report that found numerous instances when the division shared information beyond what was allowed under the law.

That included improperly sharing Social Security numbers with researchers at the University of Utah, Social Security numbers and physical characteristics with the Utah Population Database, and an individual’s physical characteristics with the state elections office — as if someone’s height, weight and eye color are relevant to voting. (The elections office said it didn’t even know it was getting that information because it had no use for it.)

Another state audit, released around the same time, found vulnerabilities in another database housing prescription drug records and the potential for doctors whose licenses had expired to access it. As with driver licenses, law enforcement also has easy access to search that database, after the ACLU lost a lawsuit trying to restrict police access.

These latest revelations about the breadth of law enforcement’s use of the database should alarm all of us. As citizens who entrusted that information to the state, we deserve answers, accountability and transparency.

The auditor’s office should conduct a thorough review of the facial recognition program and report back to lawmakers as soon as possible. Dougall has already started down that path, requesting a briefing from DPS on the scope and execution of the facial recognition program. Lawmakers should use that information to set rigorous guardrails on how citizens’ private information will be accessed in the future — not just facial recognition data housed by the driver license division, but the countless records housed in databases across the state.

Last session, legislators passed the first law in the nation requiring law enforcement to obtain a warrant to get an individual’s digital records. It’s a good example of how Utah can and should be a leader on the privacy front. Unfortunately, right now we are way behind the curve.

At the very least, law enforcement should be required to obtain an administrative subpoena to access the data, if not a warrant. There should be annual reports to the Legislature detailing law enforcement’s use of the databases and a disclosure to drivers obtaining a license about how their information will be used.

At the national level, advocacy groups have called for a complete ban on the use of the facial recognition software. Members of our congressional delegation, particularly those who, like Sen. Mike Lee, espouse a philosophy of individual liberty, should be at the forefront of this debate.

And, on a larger scale, given the massive amounts of data the state collects on citizens, Gov. Gary Herbert should appoint a chief privacy officer (apart from the privacy officer overseeing the Department of Public Safety’s data collection).

The privacy czar — or whatever they are called — can monitor what data is gathered on Utahns, ensure it is securely stored and shared, educate the public and inform lawmakers and help to formulate policies. Because Big Data is only going to get bigger, and we’ve seen why Utah needs an advocate for our rights.