Signed As Law: Vermont Bans Police Use of Facial Recognition Technology

Signed As Law: Vermont Bans Police Use of Facial Recognition Technology

by **Mike Maharrey**, *Tenth Amendment Center*
October 15, 2020

MONTPELIER, Vt. (Oct. 15, 2020) – Last week, Vermont Gov. Phil Scott signed a bill into law that bans police from using facial recognition technology. The growing movement to prohibit the use of facial recognition at the state and local levels could hinder the operation of a growing national facial recognition network.

Sen. Jeanette White (D-Putney) introduced Senate Bill 124 (S.124) back in February. The legislation makes a number of reforms relating to law enforcement, including a complete ban on the use of facial recognition technology unless it "is authorized by an enactment of the General Assembly." The law prohibits the use of facial recognition technology and the use of any information acquired through facial recognition. It does make an exception if the use of facial recognition is allowable under the state law regulating police drones – permissible only with a warrant.

The Senate passed S.124 in June by a 28-0 vote. The House approved the measure with some amendments on Sept. 22. The Senate concurred with the amendments and Gov. Scott signed the bill into law on Oct. 7.

The new law establishes the strongest limits on the police use of facial recognition in the country. ACLU of Vermont Advocacy Director Falko Schilling called it "a historic win for Vermonters' right to privacy."

> *"By enacting the broadest outright ban on police use of facial recognition in the country, Vermont has taken the lead in protecting residents' civil liberties from this invasive and inaccurate technology."*

Impact on Federal Programs

A recent report revealed that the federal government has turned state drivers' license photos into a giant facial recognition database, putting virtually every driver in America in a perpetual electronic police lineup. The revelations generated widespread outrage, but this story isn't new. The federal government has been developing a massive, nationwide facial recognition system for years.

The FBI rolled out a nationwide facial-recognition program in the fall of 2014, with the goal of building a giant biometric database with pictures provided by the states and corporate friends.

In 2016, the Center on Privacy and Technology at Georgetown Law released "The Perpetual Lineup," a massive report on law enforcement use of facial recognition technology in the U.S. You can read the complete report at perpetuallineup.org. The organization conducted a year-long investigation and collected more than 15,000 pages of documents through more than 100 public records requests. The report paints a disturbing picture of intense cooperation between the federal government, and state and local law enforcement to develop a massive facial recognition database.

> *"Face recognition is a powerful technology that requires strict oversight. But those controls, by and large, don't exist today," report co-author Clare Garvie said. "With only*

> *a few exceptions, there are no laws governing police use of the technology, no standards ensuring its accuracy, and no systems checking for bias. It’s a wild west.”*

There are many technical and legal problems with facial recognition, including significant concerns about the accuracy of the technology, particularly when reading the facial features of minority populations. During a test run by the ACLU of Northern California, facial recognition misidentified 26 members of the California legislature as people in a database of arrest photos.

With facial recognition technology, police and other government officials have the capability to track individuals in real-time. These systems allow law enforcement agents to use video cameras and continually scan everybody who walks by. According to the report, several major police departments have expressed an interest in this type of real-time tracking. Documents revealed agencies in at least five major cities, including Los Angeles, either claimed to run real-time face recognition off of street cameras, bought technology with the capability, or expressed written interest in buying it.

In all likelihood, the federal government heavily involves itself in helping state and local agencies obtain this technology. The feds provide grant money to local law enforcement agencies for a vast array of surveillance gear, including ALPRs, stingray devices and drones. The federal government essentially encourages and funds a giant nationwide surveillance net and then taps into the information via fusion centers and the Information Sharing Environment (ISE).

Fusion centers were sold as a tool to combat terrorism, but that is not how they are being used. The ACLU pointed to a bipartisan congressional report to demonstrate the true nature of government fusion centers: “They haven’t contributed anything meaningful to counterterrorism efforts. Instead, they have largely served as police surveillance and information sharing nodes for law enforcement efforts targeting the frequent subjects of police attention: Black and brown people, immigrants, dissidents, and the poor."

Fusion centers operate within the broader ISE. According to its website, the ISE "provides analysts, operators, and investigators with information needed to enhance national security. These analysts, operators, and investigators…have mission needs to collaborate and share information with each other and with private sector partners and our foreign allies." In other words, ISE serves as a conduit for the sharing of information gathered without a warrant. Known ISE partners include the Office of Director of National Intelligence which oversees 17 federal agencies and organizations, including the NSA. ISE utilizes these partnerships to collect and share data on the millions of unwitting people they track.

Reports that the Berkeley Police Department in cooperation with a federal fusion center deployed cameras equipped to surveil a "free speech" rally and Antifa counterprotests provided the first solid link between the federal government and local authorities in facial recognition surveillance.

In a nutshell, without state and local cooperation, the feds have a much more difficult time gathering information. Passage of state laws and local ordinances banning and limiting facial recognition eliminates one avenue for gathering facial recognition data. Simply put, data that doesn't exist cannot be entered into federal databases.