

King County Washington Bans Facial Recognition

Description

USA: On Tuesday, the Metropolitan King County Council unanimously passed an ordinance banning the use of 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.

Councilmember Jeanne Kohl-Welles was the lead sponsor of the ordinance. The new law prohibits county administrative offices and executive departments, including the sheriff's department, from acquiring or using facial recognition technology or facial recognition information. It also bans county agencies from issuing any permit or entering into any agreement which authorizes any third party to use facial recognition technology or obtain facial recognition information on behalf of the county.

Under the new ordinance, law enforcement agencies can still use information gathered via facial recognition in an investigation as long as they don't ask for it or produce it themselves. The law also allows the use of facial recognition in conjunction with a federal program that searches for missing children.

According to the ACLU of Washington, King County is the first jurisdiction to pass a county-wide multicity ban on the use of facial recognition.

"I think that the technology raises huge concerns, primarily on the inaccuracy of the technology, demographic biases and encroachment on civil liberties and privacy for everybody," Kohl-Welles told the *Seattle Times*. "I think it's not appropriate for us to use."

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 <u>perpetuallineup.org</u>. 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 <u>its website</u>, 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.

Image: Corbett Report

By Michael Maharrey

Date Created 06/05/2021