Maine State Police may be spying on you

Privacy advocates worry that law enforcement monitors innocent residents, and Maine is one of only two states that won't reveal whether it's using this advanced technology.

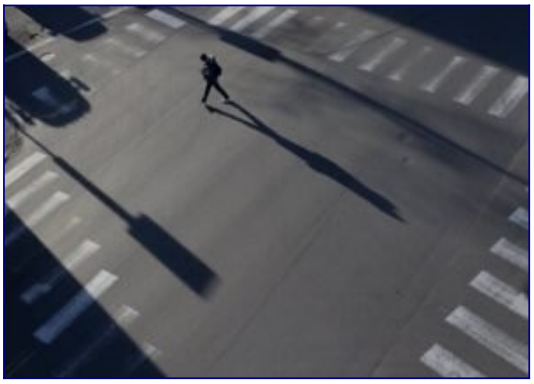
By Randy Billings Staff Writer

Public scenes like these could provide images of faces that can be scanned to identify or find people, but Maine State Police say an unusual state law means they won't tell the public whether or not they are using such technologies.

Maine State Police may be using powerful new technologies to scan your face and intercept your cellphone signals, but officials say an unusual provision in state law means police don't have to tell the public.

Government use of such technologies to investigate crimes or monitor citizens is a growing source of concern around the country and the world. And Maine's secrecy is raising alarms among privacy advocates, who worry that law enforcement could be using advanced technology to monitor residents, including those who are not suspected of any crime.

"It means the public doesn't even know what it doesn't know," said Nathan Wessler, a staff attorney with the American Civil Liberties Union's speech, privacy and technology project. "It has no idea whether there is a potential question about whether there's unconstitutional use of a surveillance technology."



A camera captures images of a pedestrian as he crosses Temple Street in Portland. *Staff photo by Derek Davis*

An investigation by the Portland Press Herald/Maine Sunday Telegram has found:

• Maine is one of two states to have a specific law, which was inspired by Cold War-era secrets kept from the Soviets, that officials say allows the state to neither confirm nor deny the use of digital technologies that might help solve crimes, but that also raises fears of abuse, privacy violations and the surveillance of citizens.

• Despite evidence that the Maine State Police has worked for years with federal agencies to develop its use of digital surveillance technology, the agency now uses that law to refuse to answer any questions about such efforts, or even acknowledge that they exist.

• The secrecy about investigative or surveillance technology extends to the Maine Information and Analysis Center – a so-called fusion center that brings the state police together with other federal and state agencies to foster information sharing and does not reveal its activities.

• The state police, and its partners in the fusion center, may soon have access to Mainers' Real ID photos, which are especially suited for face-scanning technology. State law currently prohibits use of license photos for facial recognition searches, but a bill now moving through the Legislature would allow state officials to conduct such searches and provide information to outside law enforcement agencies.

The lack of disclosure prevents public oversight to ensure that people's privacy and constitutional rights are being respected. Advanced technologies make it possible for authorities to conduct mass surveillance, including collecting cellphone information and comparing the images of suspected criminals against databases of people who are not suspected of committing any crimes. The technology can track people's movements and help determine groups and individuals with whom a person associates.

And the lack of transparency does not allow the public to know whether the government is being a good steward of tax dollars.

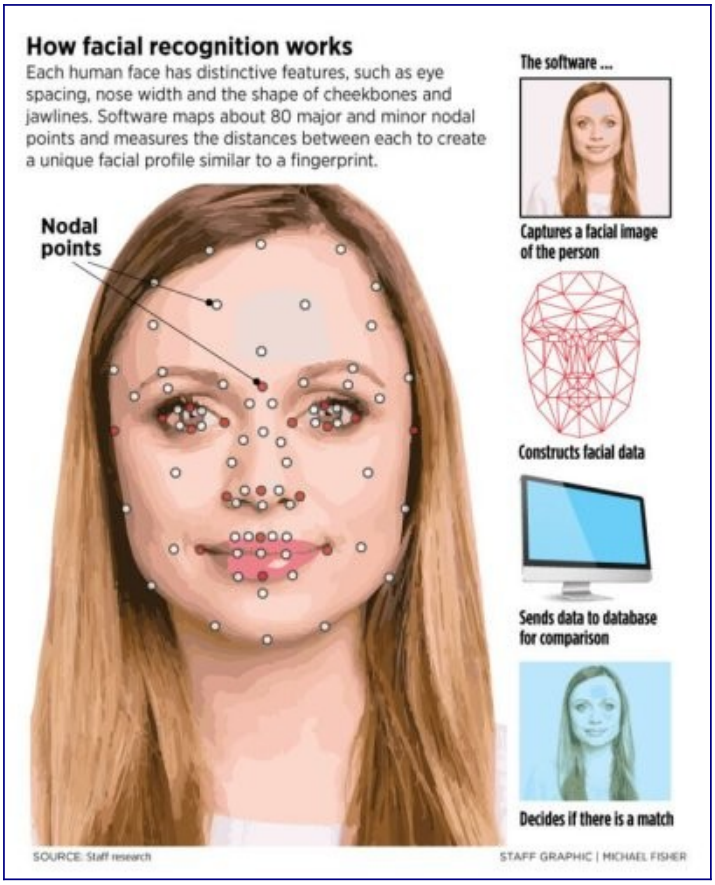
"It's just an extremely broad power of secrecy," said Wessler. "It just completely hobbles the opportunity for public debate on very important subjects."

"It's a per se mandate on the agency to clam up even before the process gets going," he added. "And that, I think, is particularly pernicious and dangerous to our tradition of democratic government, because it cuts transparency completely off at the knees."

POWERFUL NEW TOOLS

The lack of disclosure comes as communities across the United States are trying to regulate technology that allows local law enforcement to conduct sweeping surveillance of the public, including people who are not suspected of crimes.

Police departments are getting more sophisticated as technologies originally designed to enhance national security are deployed to state and local police departments to solve everyday crimes. And in some cases it's being done without a robust public discussion about what limits, if any, should be placed on its use.



Two types of surveillance technology have come under the most scrutiny from civil liberties advocates and elected officials: facial recognition and cell site simulators. Both are capable of gathering large caches of personal information.

Brendan McQuade, an assistant professor of criminology at the University of Southern Maine who has written a book about secretive fusion centers, said the government has the ability to gather vast amounts of information using a variety of technology, including software to monitor social media, E-ZPasses used to pay highway tolls, and automated license plate readers, among others.

“The fact that we don’t know what agencies have what technology, I think, should be very troubling,” McQuade said. “They’re bought in secret. They’re used in secret. And unless there’s concerted political action and legislative actions, there’s nothing preventing police departments from doing very aggressive, warrantless surveillance.”

Facial recognition technology can map an individual’s face using a high-resolution digital image or surveillance video and then compare that image to an existing database of known people.

It works by essentially mapping a person’s dominant facial features, such as eye shape and spacing, as well as jaw and nose lines. The software measures the distances between dozens of reference points, creating a unique profile similar to a fingerprint. The profile is then compared to the faces in existing databases, such as those that contain driver’s licenses, state IDs, immigration records, passport photos or police mug shots.

A surveillance camera positioned at the intersection of Cumberland Avenue and Elm Street in Portland. *Staff photo by Derek Davis*

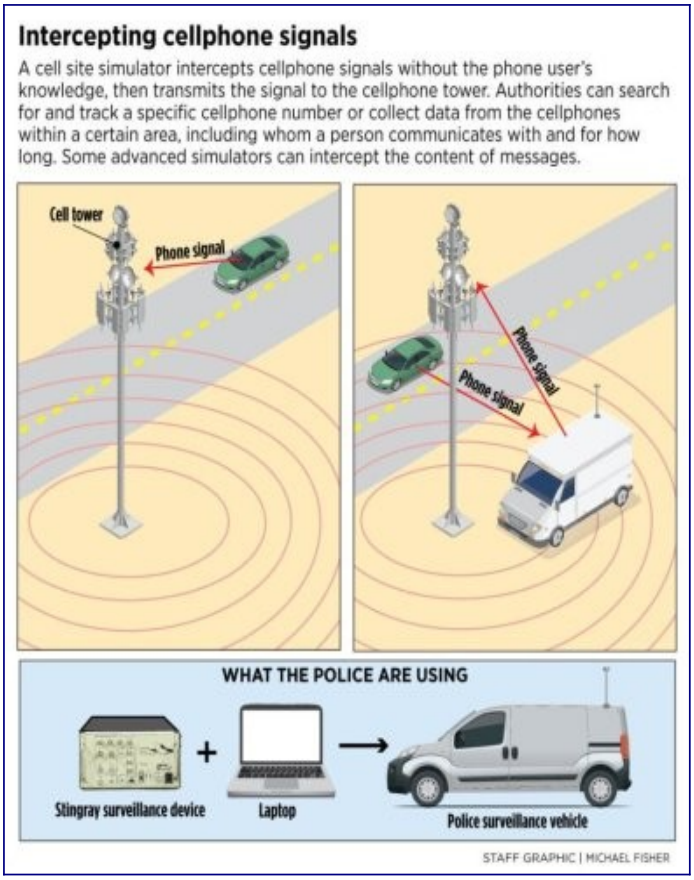
More advanced programs can also conduct an analysis of skin texture to increase accuracy and, in some cases, account for different facial expressions, facial hair or eyeglasses. Some technology can provide real-time identification of people captured on video.

The New York Times recently reported that more than 600 local police agencies are using a new facial recognition cellphone app created by the private company Clearview AI to search a cache of 3 billion images scraped from such sites as Facebook, Venmo and YouTube to identify potential suspects.

Other technological tools used by police include cell site simulators, also known as IMSI catchers or Stingrays, that can essentially turn the cellphone you carry into a real-time tracking device.

A cell site simulator can be the size of a briefcase and carried in a police cruiser or on an airplane to ping cellphones. It sends out a signal that tricks nearby cellphones into connecting with the simulator, rather than a cellphone tower. The signal is then passed to a tower, and it happens without the user knowing.

Authorities can either search for and track a specific cellphone number or collect data from all of the cellphones within a certain area. That data can include the IMSI – or International Mobile Subscriber Identity – and metadata about whom a person communicates with and for how long. And some advanced simulators can intercept the content of messages, according to the Electronic Frontier Foundation.



Groups including the ACLU have raised concerns about both forms of technology, saying that widespread use infringes on constitutional rights that protect people from unlawful searches and guarantee the right to peacefully assemble and associate with groups of people.

Privacy advocates point to China as an example of the dangers posed by unrestricted use of such technologies. The Chinese government is using facial recognition to monitor and oppress the Uighurs, a largely Muslim minority ethnic population. China is also working on technology that can identify people by the way they walk, so that they can be tracked even if their faces are obscured. The New York Times reported that Chinese officials are using the technology to shame people who wear pajamas in public, for example, while police in London are going to use it to identify people captured on video in real time.

McQuade is among those concerned.

“It’s akin to having close personal surveillance on someone for a long time and reading their diary about who they’re calling and who they’re visiting,” he said.

A handful of communities in the United States have restricted or banned the use of facial recognition technology, both because of constitutional concerns and a high error rate when trying to identify people of color and women. The state of California has enacted a three-year ban on using facial recognition in conjunction with cameras worn by police officers.

A study published in December by the National Institute of Standards and Technology found the rate of false positive identifications, which could make an innocent person a criminal suspect, occurred 10 to 100 times more frequently among African-Americans and Asians than with Caucasians. The study tested 189 algorithms from 99 developers to compare photos in four federal databases containing 18.27 million images of 8.49 million people.

In Portland, the City Council has twice postponed a vote on a proposal from City Councilor Pious Ali that would prohibit city officials, including its police force, from obtaining, retaining, accessing or using any facial recognition technology or information provided by such technology.

The proposed ban comes as Maine's largest city has embraced so-called smart-city technology, which includes traffic monitoring and has stoked fears about government's increasing ability to watch over citizens. And Portland's police officers are now equipped with cameras mounted on their chests to capture video of each person an officer interacts with, another source of concern about privacy.

Portland City Hall has been equipped with surveillance cameras that videotape people inside the building and can also record audio. *Staff photo by Brianna Soukup*

Portland's smart-city efforts so far include LED streetlights that can double as WiFi routers, and sophisticated traffic management systems that can read and adjust signals in response to real-time traffic. Portland officials have expressed interest in other "public safety functions," but so far, officials say that has not included facial recognition technology.

City officials, including Police Chief Frank Clark, said they are not currently using facial recognition technology and opposed restricting any future use of technology that might enhance public safety. The chief said he would alert the city manager or the council if the department ever planned to use it.

Clark highlighted the technologies' potential to help solve crimes and identify exploited children, crime victims and people suffering from dementia.

"While we do not have any immediate plans to acquire facial recognition, I am an advocate of taking advantage of contemporary 21st century technologies to drive better public safety outcomes," Clark said in a memo to councilors, adding that strong policies can prevent misuse and infringement on constitutional rights. "A ban on facial recognition technology would only take away a potential tool that is helping to increase efficiencies and provide assistance for crime victims and people in crisis in other jurisdictions."

And the city also has said it does not use any cell site simulators. A request for internal public records pertaining to the technology produced no relevant documents, a city spokesperson said.

Cumberland County Sheriff Kevin Joyce has said his agency began using facial recognition technology in 2012 to search its database of mug shots to identify people who refused to give their names or were suspected of having fake IDs. Joyce said they stopped using the technology because it only worked when the photo of a subject's face was taken at the correct angle and in good lighting.

While both the Portland police chief and the Cumberland County sheriff have been willing to talk about whether the technology is in use, the Maine State Police are not as forthcoming.

GLOMAR: COLD WAR SECRECY

The Portland Press Herald/Maine Sunday Telegram requested a range of public documents relating to facial recognition technology and cell site simulators from the Maine State Police under Maine's Freedom of Access Act. The documents included any requests for proposals, contracts, payments, policies governing usage, evaluations of the technology and communications about the use of such technology.

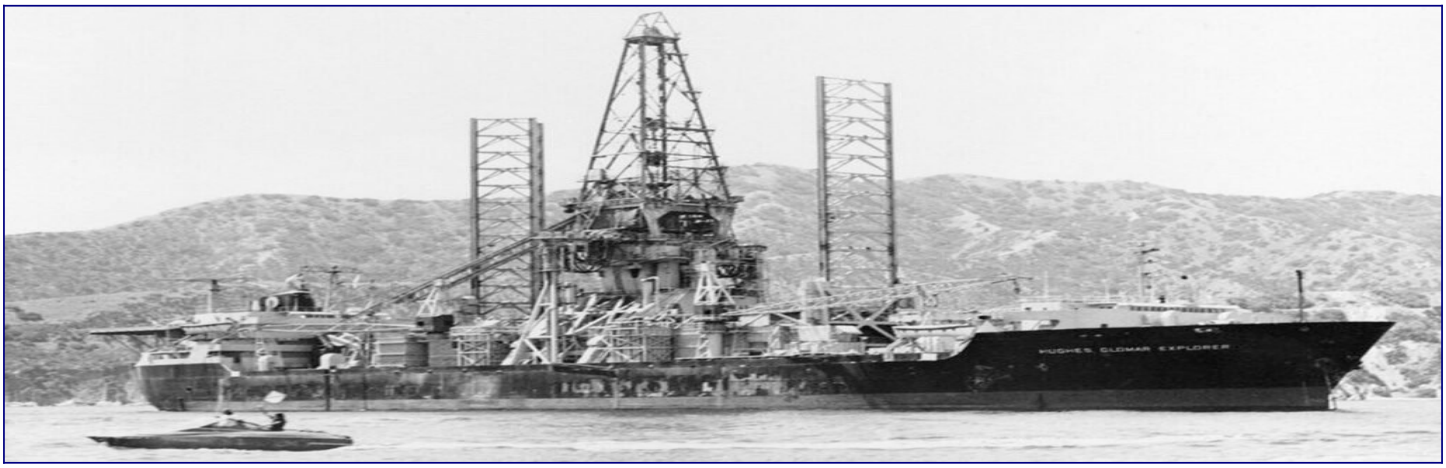
Christopher Parr, staff attorney for the Maine State Police, issued formal denials to both requests, citing a provision of Maine law enacted in 2013 that appears to be unique in the United States.

"Answering your inquiry would require us to confirm the existence or nonexistence of records and information relating to the type of technology that is the subject of your email," Parr said in November. "As a matter of law, we are unable to confirm the existence or nonexistence of such records and information."

Sigmund Schutz, an attorney for the Press Herald and Telegram, is challenging that interpretation and asking the state to reconsider its denial. He noted that the request does not pertain to a specific investigation or person, nor does it pertain to a type of technology that is unknown to the public.

"Based on the nature of the records sought, it is not plausible that disclosure of any or all of the requested records would cause any of the harms that would warrant confidentiality," Schutz wrote.

Parr's response to records requests is often referred to in legal circles as a Glomar, a non-answer created by the Central Intelligence Agency in the 1970s in response to public inquiries about a covert operation to recover a sunken Soviet submarine.



The Hughes Glomar Explorer off the coast of Catalina Island, Calif., in August 1975, about a year after the ship took part in a secret attempt to recover a sunken Soviet submarine. The ship's name is short for Global Marine, a company owned by Howard Hughes at the time. When the Central Intelligence Agency was asked about the covert mission, it said it could neither confirm nor deny the existence of the effort, an answer that is now known as a Glomar response. *AP*

After a Soviet submarine mysteriously sank in 1968, the U.S. located the disabled sub and launched a covert mission to retrieve it, believing it contained nuclear missiles or nuclear codes, or both. The U.S. hired the Global Marine company, which was owned by Howard Hughes, to build a special ship to try to retrieve the sub. The ship was named the Hughes Glomar Explorer.

The U.S. was unable to surface the sub. Once news began to spread about the failed mission in 1975, the Central Intelligence Agency drafted a response that was truthful without confirming or denying the existence of the covert operation.

The response became known as Glomar.

MAINE'S SECRECY STANDS OUT

The ACLU says Maine is one of only two states to give law enforcement the ability in state statute to neither confirm nor deny a broad range of public records relating to investigatory methods and technologies.

Wessler, the ACLU staff attorney, said Maine's law is more sweeping than a similar law in Indiana, the only other state he's found to have codified a Glomar response in state law. He said Indiana's law requires proof that disclosing the information would harm an investigation or an individual, whereas Maine's does not.

"In Maine, it doesn't have to hurt anybody," Wessler said. "It could be information that's completely in the public interest and that wouldn't interfere with any law enforcement investigation and the police department still has to withhold any mention of whether they have documents or don't have documents."

The state police interpretation of the statute highlights what may be an unintended consequence of a 2013 rewrite of state laws pertaining to criminal history records and intelligence and investigative materials.

Louis Pfeifle fills out paperwork for a Real ID-compliant driver's license in January at the Bureau of Motor Vehicles in Portland. *Ben McCanna/Staff Photographer*

It's only one line in a 20-plus-page rewrite, but it has broad implications on the public's ability to understand the type of technologies police are deploying, the cost of that technology and what policies are in place to prevent misuse.

A section titled "Confirming the existence or nonexistence of confidential intelligence and investigative record information" states: "A Maine criminal justice agency may not confirm the existence or nonexistence of intelligence and investigative record information confidential under section 804 to any person or public or private entity that is not eligible to receive the information itself."

A review of the legislative file does not suggest that section of the bill received much discussion. It was pitched as a way to clarify and improve an existing law.

Marc Malon, the legislative and press liaison for the Maine Attorney General's Office, referred all questions about the 2013 law change to Charles Leadbetter, a retired assistant to the attorney general who was the point person for the rewrite.

Leadbetter said in a brief interview that the lengthy summary of the bill spoke for itself. That summary says that section of the law had no previous counterpart, but was modeled after a similar provision intended to protect confidential information about a specific person.

Malon did not respond to requests to speak to any other officials in the AG's office and whether state police were interpreting the law correctly.

Representatives of Gov. Janet Mills, who was the attorney general in 2013, did not respond to interview requests. And Public Safety Commissioner Michael Sauschuck requested that questions be submitted in writing and has yet to respond to questions sent on Jan. 22.

Maine's sweeping use of that exemption is raising concerns among civil liberties advocates.

McQuade, the assistant professor, said the lack of disclosure prevents any meaningful oversight of the technology and allows law enforcement to establish a pattern of behavior before lawmakers and the public can have a discussion about whether or even how to use it. And any policies that come after the fact can be greatly influenced by the pattern of behavior already established, he said.

"We see how police practice actually molds the law," McQuade said. "It should be very threatening if you take the Constitution seriously. This is a big imbalance of power that gives the executive branch powers that are reserved on paper for the legislative bodies."

Clare Garvie, a researcher at Georgetown Law's Center on Privacy and Technology, said that only two states would neither confirm nor deny use of facial recognition technology while she was conducting research for a 2016 report titled "The Perpetual Line-up: Unregulated Police Face Recognition in America." Those states were Maine and Massachusetts, she said.

That study, which sought records from 106 law enforcement agencies, found that 26 to 30 states allow law enforcement to run or request searches against their driver's license and state identification databases and roughly one in two American adults have their photos searched this way. Despite the state's refusal to provide information, Maine was listed as being capable of searching FBI mug shots – information gleaned from a U.S. Government Accountability Office report.

Wessler, of the ACLU, said privacy advocates got a similar response while researching the use of cell site simulators by law enforcement agencies throughout the country. Wessler said that only Maine and the U.S. Fish and Wildlife Service would neither confirm nor deny the use of cell site simulators in response to public records requests from either the ACLU, privacy researchers or the press.

Both technologies have been the subject of inquiry by the GAO, which has generally called for more transparency and more privacy protections for innocent civilians.

"Police departments have a lot of power and we expect them to use that power responsibly to protect us," Wessler said. "But American history is replete with examples of abuses by police and that's why there needs to be strong oversight and transparency into their practices."

SIGNS POINTING TO USE

Despite the secrecy, there is evidence Maine may be using some of this technology.

Three years ago, Parr, the state police attorney, acknowledged in emails with Georgetown Law researchers that the agency was working with the FBI to conduct "considerable testing" of facial recognition technology.

The acknowledgement came five months after Maine had been listed in a 2016 report by the GAO as one of seven states to have an agreement with the FBI to conduct facial recognition searches on its federal database. The other states were Florida, Maryland, Michigan, New Mexico, Texas and Arkansas.

The report – "Facial Recognition Technology: FBI Should Better Ensure Privacy and Accuracy" – said Maine was one of 15 states plus the District of Columbia that had the technical ability to conduct facial recognition searches of the FBI's Next Generation Identification-Interstate Photo System. That database has over over 90 million civil and criminal photos and images of scars, marks and tattoos, according to a follow-up report in 2019. Of the 93 million photos, 38 million were criminal photos. And law enforcement has the ability to add photos of unknown individuals who are part of a federal investigation.

Maine State Police entered into an agreement to search that database back in 2012. The 2016 GAO report states that from the beginning of the pilot program in 2011 through 2015, search requests from each participating state ranged from under 20 by one state to 14,000 by another state. The report does not say how many search requests came from Maine.

In response to public records requests submitted by Georgetown Law's Center on Privacy and Technology, Parr told researchers that Maine was currently testing the technology, but had made no decision about how or whether to use it in the future. His response came after both the GAO and the Georgetown reports were published.

"For some time Maine has been working with the Federal Bureau of Investigation, Criminal Justice Information Systems Division to implement the use of facial recognition technology," Parr wrote. "Although at this point we technically are capable of using the technology, we have been in no hurry to do so without considerable testing, which we still are conducting."

More than three years later, it is still not clear to what extent Maine is searching this database and what policies guide those searches.

At the time, Parr noted that the state had received the FBI's policy and implementation guide and that the state would likely draft its own. In 2018, Parr told researchers that the state's position had not changed.

But, in 2019, Parr told the Press Herald and Telegram even less.

"As a matter of law, we are unable to confirm the existence or nonexistence of records or information responsive to the request. See 16 M.R.S.A. § 807," Parr wrote.

Knowing whether state police are using facial recognition could become more important this year.

Maine is in the midst of rolling out new driver's licenses and state identification cards that are compliant with the federal Real ID program – a move that could greatly expand the number of photos that can be searched using facial recognition.

USE OF FACIAL RECOGNITION FOR REAL ID

Beginning in October, Mainers will need to have a Real ID or a passport if they want to board an airplane or enter a secure federal facility. Getting that form of identification requires a photo that can be more effectively used in a facial recognition system. That could greatly expand the number of photos law enforcement can search.

Real ID photos are especially suited for facial recognition searches, because of their high resolution. In 2017, the state said "Real ID applicants must … submit to a photograph using facial recognition technology."

Lee Bumsted of South Portland proofreads her driver's license information after being photographed Tuesday for a Real ID-compliant driver's license by Bureau of Motor Vehicles manager Lisa Anderson, left, in Portland. *Ben McCanna/Staff Photographer*

And while Maine law currently prevents state officials from outside agencies, including the FBI, from searching its database, an effort is underway to change that.

A bill submitted by the Secretary of State's Office, which oversees the Bureau of Motor Vehicles, would allow the bureau's investigators to conduct searches of its Real ID database for outside agencies.

Secretary of State Matt Dunlap said his office is still developing rules for conducting those searches. But he said the state would continue to prohibit outside agencies, such as the FBI, from having open-ended access to the database.

"Nobody is going to have wholesale access to the database," Dunlap said. "We've never allowed that and we're not proposing it now."

Dunlap said the bill is intended to allow the BMV to help police identify specific individuals.

Dunlap cited a police standoff as an example. Police could provide the BMV with a person's name and other information, and the BMV would provide police with a license photo so they can locate the correct person. It's a practice that occurs with the old license system, he said.

Dunlap said the state "would never" allow an outside agency to search the database to identify individuals who were captured on camera attending a public rally or demonstration.

However, the Real ID system and the proposed legislation would open up a new avenue of searches by allowing police to submit a photo of an unknown person to the BMV so it can run a facial recognition search in hopes of digging up a positive ID. That would essentially put anyone who has a Real ID into a virtual lineup.

Dunlap said those types of searches could be allowed under certain circumstances if the bill passes. But he stressed facial recognition alone is not enough to establish a positive identification and that additional verification is needed.

“You don’t ascertain identity with only one element,” he said.

The bill, L.D. 1899, "An Act to Amend Certain Motor Vehicle Laws," received a public hearing on Jan. 23 before the Legislature's Committee on Transportation.

Michael Kebede, policy counsel for the ACLU of Maine, spoke in opposition to the bill as drafted. He asked the committee to consider an amendment that would restrict facial recognition searches only to emergency situations where there is an imminent threat to life.

Kebede said the technology poses "grave risks" for black people, especially black women, transgender people and immigrant communities, because it misidentifies these groups at higher rates than it does Caucasians.

"Persistent identification and tracking can have a chilling effect, as people will be less likely to exercise their rights if they know the government is tracking and identifying them everywhere they go," Kebede said. "Mainers must be able to visit substance use clinics, churches and synagogues, friends and family, political protests and doctors' offices without fear that a government agent is secretly keeping tabs on their every movement."

During a Feb. 6 work session, the Transportation Committee amended the bill to include the ACLU of Maine's amendment, as well as requiring the BMV to draft "major substantive rules for other authorized uses of facial recognition technology."

Dunlap said he shares the concerns of privacy advocates who worry about misuse. The state resisted complying with the Real ID program for years, he said, but lawmakers changed course when the federal government announced that people would no longer be able to fly on a commercial airliner or enter a federal building without a non-Real ID-compliant form of identification or passport.

He said that each time the database is searched, it logs a record of who searched it and when. It's unclear whether those records would be public because the rules are still being considered.

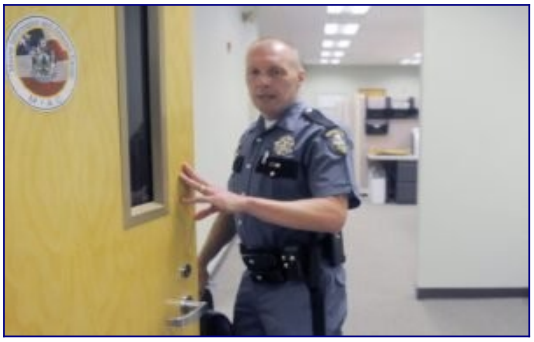
"Facial recognition really scares a lot of people and I think it really should," Dunlap said. "I think people have good reason to be freaked out about that."

Although Dunlap stressed that searches could only be conducted by BMV staff on behalf of other agencies, those employees already work closely with other federal, state and local law enforcement officials.

The BMV is one of 12 agencies that provide staffing and support for the Maine Information and Analysis Center, one of roughly 80 so-called fusion centers created in the wake of the 9/11 terrorist attacks whose specific activities are also kept under wraps.

FUSION CENTER

Maine State Police oversee operations at the Maine Information and Analysis Center.



In this 2016 photo, Lt. Scott Ireland opens a door at the Maine Information and Analysis Center at the Department of Public Safety in Augusta. *Staff photo by Andy Molloy*

The center's 12-member staff includes federal, state and local officials, among them representatives of the FBI, U.S. Customs and Border Protection and the BMV, which is building a database that could be searched with facial recognition technologies through the Real ID program.

Its activities are overseen by a 12-member advisory board. It includes one civilian and a private attorney, while the other 10 members include four members from the Maine State Police, Attorney General Aaron Frey, Douglas Farnham, adjutant general of the Maine National Guard, and a representative from Central Maine Power Co. Maine State Police Lt. Michael Johnston, the fusion center's director, said that a CMP representative is on the board because part of the center's mission is to protect critical infrastructure, including utilities.

This photo taken on Friday Sept. 4, 2015 shows the Maine Department of Public Safety, home of the so-called fusion center. *Photo by Joe Phelan*

Little is known about the activities of Maine's fusion center. Its investigations involve counterterrorism, felony drug crimes, violent crimes, including domestic violence, and property crimes, among others, Johnston said.

Johnston would not say what types of technologies are available to state and local police agencies, which submit daily inquiries to the center, and he would not provide a detailed budget, meeting minutes from an advisory committee tasked with oversight, or any audits of the center's operation without first conferring with Parr, the attorney. Parr has not yet indicated whether any documents would be released in response to the request.

Johnston said the center receives inquiries from local police and other agencies on a regular basis. But he would not point to any cases in which the information or the analysis from the center helped apprehend a suspect.

"We have small victories every day," he said. "We're just a piece of the puzzle."

When asked about protecting citizens' privacy, Johnston said the fusion center operates within the constraints of the Constitution, as well as state and federal laws, policies and directives. The center is assessed annually by the U.S. Department of Homeland Security and undergoes a regular audit, as well as being overseen by the advisory board, which is supposed to meet at least once a year.

Those audits and other records, however, were not immediately available.

The center's privacy policy is online. It does not reveal what types of technologies are used at the center, but it does lay out the ground rules for acquiring, storing and retaining information.

The policy states that the center may only seek, acquire and retain information that relates to a possible threat or criminal predicate, based on reasonable suspicion and that comes from a reliable source, among other requirements. However, it also states that the center "may retain information that is based on a level of suspicion that is less than 'reasonable suspicion,' such as tips and leads or a suspicious activity report."

The policy says that methods of acquiring information must be legal and the center shall not directly or indirectly seek, acquire or retain information from a nongovernmental partner if it suspects that partner is legally prohibited from having or disclosing that information, acquired that information through a method that the center itself could not legally use, or if the information itself could not be legally obtained by the center. Outside partners must certify in writing that they comply with laws and their methods are not based on misleading information-gathering practices.

"There are multi-layers of oversight for the fusion center," Johnston said. "While we're protecting them (citizens) from physical threats and harms, we have to make sure we're protecting their civil rights and liberties and that we're balancing the two."
