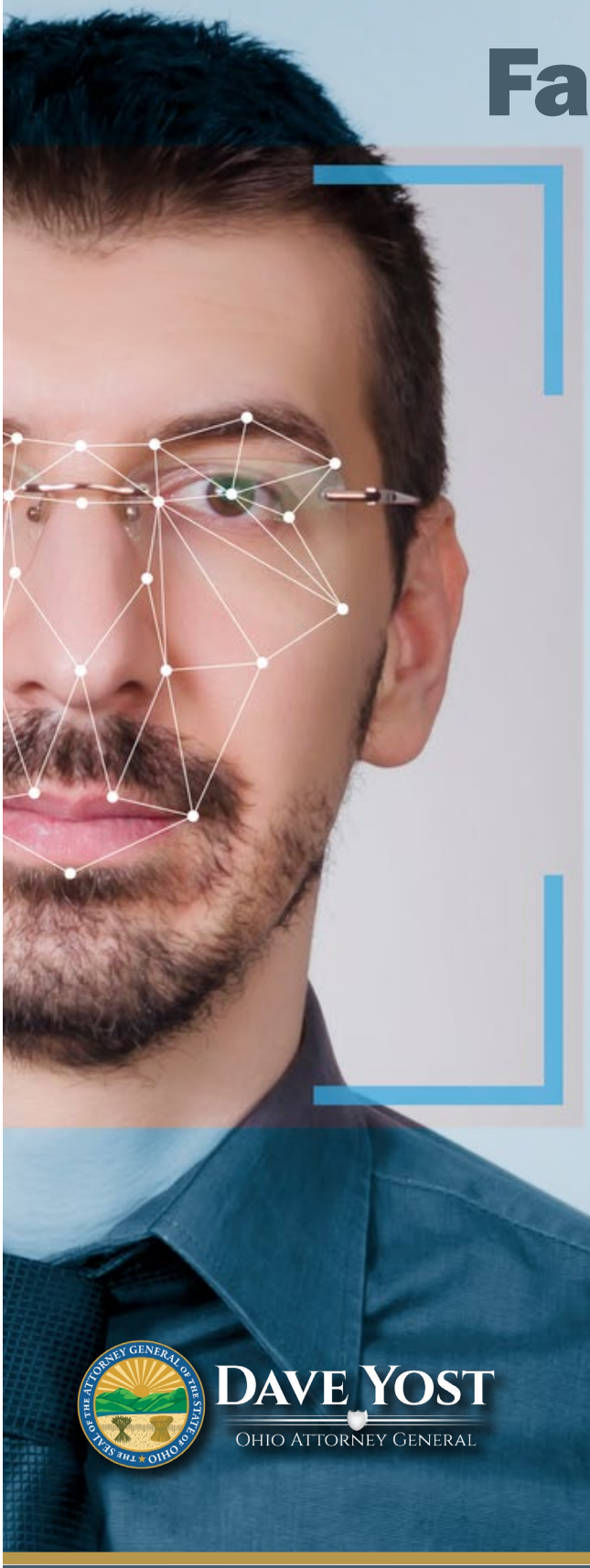
PROTECTING ★ THE ★ UNPROTECTED

Facial-Recognition Inquiries

A Special Report

Whether accessed by local, state or federal law enforcement, Ohio's facial-recognition database is used only for crime-fighting and is protected by limited access, strict rules and regular oversight.



DAVE YOST
OHIO ATTORNEY GENERAL

Executive Summary

In early July, The Washington Post published a story headlined "FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches."

The story asserted that the Federal Bureau of Investigation and Immigration and Customs Enforcement "have turned state driver's license databases into a facial-recognition gold mine, scanning through millions of Americans' photos without their knowledge or consent…"

It also asserted that federal agencies have "turned state departments of motor vehicles databases into the bedrock of an unprecedented surveillance infrastructure."

Although Ohio was not named in the story, the next day The Columbus Dispatch published a story outlining Ohio's facial-recognition database and noting that it had been used by federal agencies.

Ohio's facial-recognition database is just one of 22 applications and data sets that are part of an online search system called the Ohio Law Enforcement Gateway, or OHLEG. This is an electronic information network that allows law enforcement agencies and related criminal justice agencies to share criminal justice data efficiently and securely. Its purpose is to help these agencies investigate and prevent crime. It is operated by the Bureau of Criminal Investigation, a division of the Ohio Attorney General's Office.

Following these newspaper stories, Ohio Attorney General Dave Yost directed his staff to review the state's facial-recognition system to detail how it is used, what safeguards prevent abuse and who has access to the technology. This report is the result of that review.

Summary of the results of the Ohio Attorney General's review

The key finding of the review is that federal agency searches of Ohio's facial-recognition database constitute just 3.8 percent of all facial-recognition searches conducted since 2017. All were conducted in accordance with stringent OHLEG requirements and safeguards limiting searches to legitimate criminal justice purposes. There is no evidence of federal misuse of the facial-recognition database, such as for mass surveillance, broad dragnets or other illegitimate uses.

Other findings of the review include:

- Ohio's facial-recognition technology is strictly controlled through OHLEG, which provides criminal justice agencies access to a wide variety of databases containing information vital to the investigation of crime and missing persons. One of those databases is the facial-recognition database.
- OHLEG is used only for criminal justice purposes. Those with access include local and state law enforcement agencies, federal law enforcement agencies, courts, and government agencies that include divisions with investigative powers, such as an inspector general.
- All users of the facial-recognition portion of OHLEG are Ohio-based or, in the case of federal agencies, have offices in Ohio. There are no out-of-state users of the facial-recognition system.
- Access to the facial-recognition database is more restricted than that for other OHLEG databases and is available only to those who demonstrate a specific need.
- Currently, there are 52,680 OHLEG user accounts. However, 15,382 of these accounts have a status of *disabled* because they have not logged in for 120 days. To regain access, these users would have to complete a new application. An additional 11,740 users are *suspended* because they have not logged in for 90 days. To regain access, they would have to contact OHLEG to reset their password. This leaves 25,558 active user accounts, 4,549 of which have facial-recognition access.
- Every user of the facial-recognition system must have an approval from his or her agency head before being assigned a unique log-on, and all searches must be conducted for a legitimate law enforcement purpose under strict guidelines. Each search is recorded for review.
- OHLEG use, including the facial-recognition database, is audited by Ohio Attorney General auditors and by independent outside auditors to ensure that the system is not being abused.
- The OHLEG facial-recognition database contains 24 million images. More than 21 million of these images were supplied by the Ohio Bureau of Motor Vehicles in 2013. All of the BMV images date from 2011 and earlier, with no new BMV

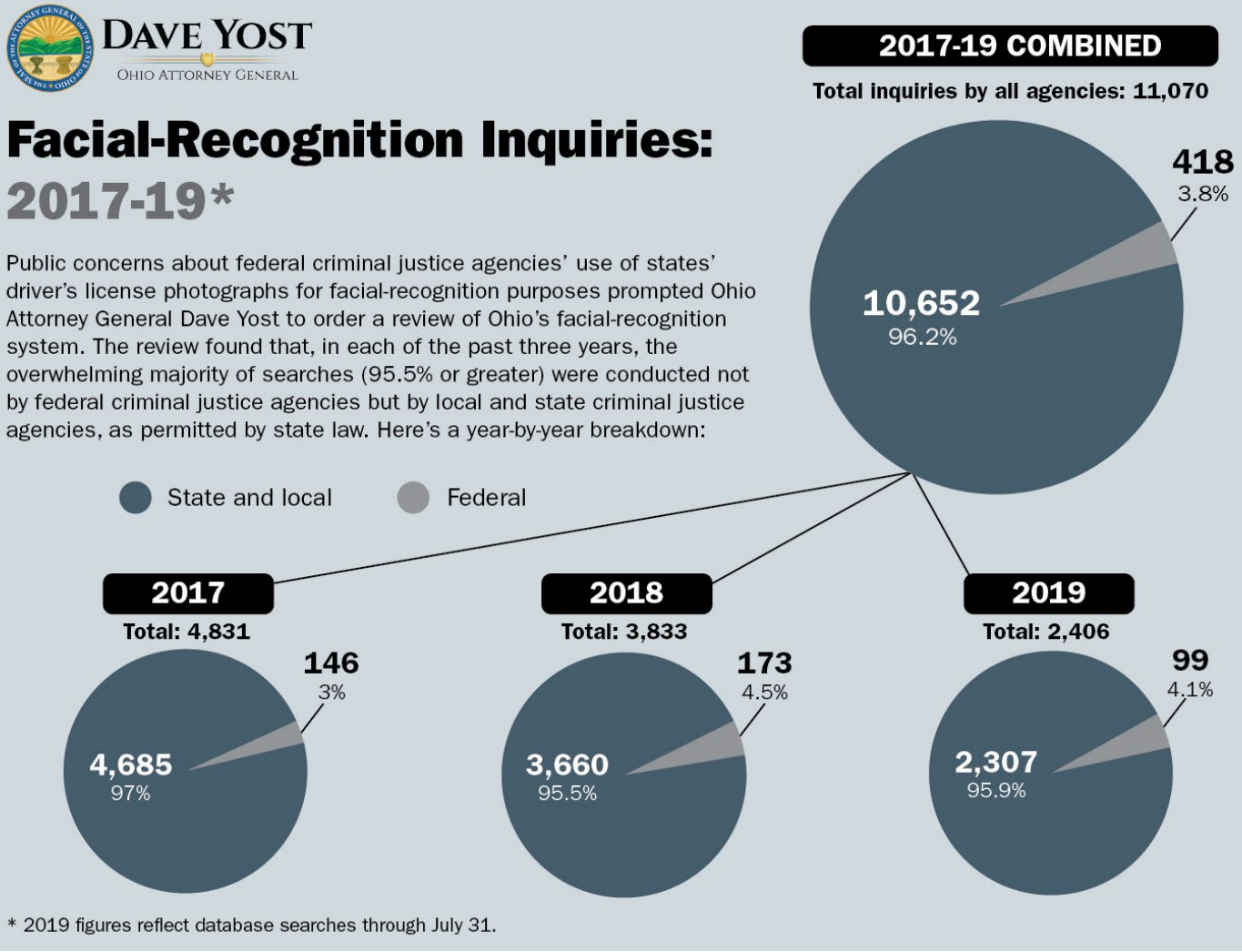
images added since. An additional 2.4 million images were supplied by the Ohio Supreme Court/Ohio Courts Network. The remainder came from various Ohio law enforcement agencies and from the Ohio Department of Rehabilitation and Correction.

- The use of photos from the Ohio Bureau of Motor Vehicles for law enforcement purposes is authorized under state and federal law.
- Federal agencies that have used Ohio's facial-recognition database include the U.S. Border Patrol; U.S. Department of State Bureau of Diplomatic Security; U.S. Immigration and Customs Enforcement; the FBI; Federal Reserve Bank of Cleveland; Drug Enforcement Administration; the U.S. Marshals Service; and the Bureau of Alcohol, Tobacco, Firearms and Explosives; and others.

DAVE YOST
OHIO ATTORNEY GENERAL

Facial-Recognition Inquiries: 2017-19*

Public concerns about federal criminal justice agencies' use of states' driver's license photographs for facial-recognition purposes prompted Ohio Attorney General Dave Yost to order a review of Ohio's facial-recognition system. The review found that, in each of the past three years, the overwhelming majority of searches (95.5% or greater) were conducted not by federal criminal justice agencies but by local and state criminal justice agencies, as permitted by state law. Here's a year-by-year breakdown:



* 2019 figures reflect database searches through July 31.

From Jan. 1, 2017 until July 31, 2019, Ohio's facial recognition database was accessed for 11,070 searches, including:

2017

4,831: Total inquiries by all agencies

4,685: Total inquiries by state and local agencies (97%)

146: Total inquiries by federal agencies (3%)

The 146 federal total includes:

59: Immigration and Customs Enforcement

43: State Department/Bureau of Diplomatic Security

37: FBI Dayton, 32; FBI Cincinnati, 5

3: Bureau of Alcohol, Tobacco and Firearms, Columbus

3: U.S. Marshals Service

1: NASA Glenn Research Center/ Office of Protective Services

2018

3,833: Total inquiries by all agencies

3,660: Total inquiries by state and local agencies (95.5%)

173: Total inquiries by federal agencies (4.5%)

The 173 federal total includes:

97: U.S. Border Patrol-Sandusky Bay Station

32: State Department/Bureau of Diplomatic Security

21: Immigration and Customs Enforcement

6: FBI Columbus

6: U.S. Marshals Service: Columbus, 3; Akron, 2; Cleveland, 1

5: Drug Enforcement Administration: Toledo, 4; Columbus, 1

4: Federal Reserve Bank of Cleveland

2: Bureau of Alcohol, Tobacco and Firearms, Columbus

2019 *(through July 31)*

2,406: Total inquiries by all agencies

2,307: Total inquiries by state and local agencies (95.9%)

99: Total inquiries by federal agencies (4.1%)

The 99 federal total includes:

47: U.S. Border Patrol, Sandusky Bay Station

36: Immigration and Customs Enforcement

15: State Department/Bureau of Diplomatic Security

1: U.S. Marshals Service

What is facial-recognition technology?

Facial-recognition technology is software that digitally maps facial features from a photograph or video and uses that data to recognize those same facial features in a different photo or video. With this technology, a photo of an unidentified person can be digitally compared with those in a database of identified images to seek a match.

The accuracy of this technology is rapidly improving, and facial recognition is being applied in a variety of ways. Retailers can use facial recognition to watch for known shoplifters. Similarly, schools could use facial recognition to spot expelled students and other unwanted visitors trying to enter school property.

Apple's latest iPhones use facial recognition to unlock the phones. Social media platforms such as Facebook use facial recognition to identify photos in which Facebook users appear and to help tag them. Airlines have started to use facial recognition to help speed baggage handling, flight check-in and boarding. Such uses are likely to spread, such as for verifying the identity of ATM users.

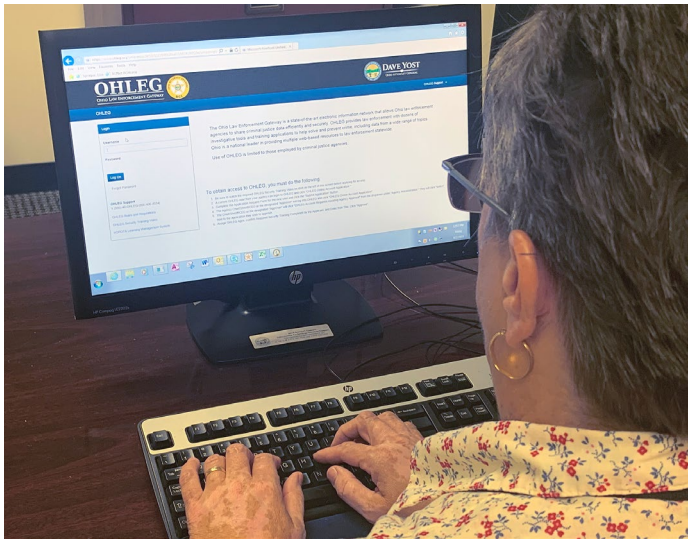
For law enforcement, facial recognition has a variety of applications. For example, if a video surveillance camera in a bank captures an image of a bank robber, that image can be compared with those in a database of identified images in the hope of finding a match that identifies the perpetrator. The technology also can be used to spot missing persons, abducted children and victims of human trafficking, and to help with cases of identity theft.

Although the technology has many positive uses, it also provokes concerns about privacy and government surveillance. For example, the People's Republic of China is making growing use of facial recognition to monitor members of disfavored ethnic groups and political opponents.

These concerns are legitimate, so it is vital that facial-recognition use by government be conducted only for legitimate purposes and with stringent security to prevent abuse.

Ohio's system comports with state and federal law and has stringent safeguards limiting access and use of all OHLEG data sets, including the facial-recognition database.

OHIO LAW ENFORCEMENT GATEWAY (OHLEG)



Ohio Revised Code Section 109.57(C)(1) provides that the superintendent of BCI may operate a center for electronic, automated, or other data processing for the storage and retrieval of information data and statistics pertaining to criminals and to children under 18 years of age who are adjudicated delinquent children for committing an act that would be a felony or an offense of violence if committed by an adult, criminal activity, crime prevention, law enforcement and criminal justice.

ORC Section 109.57(C)(1) goes on to provide that the superintendent may establish and operate a statewide communications network to be known as the Ohio Law Enforcement Gateway (OHLEG). The purpose of this network is to gather and disseminate information, data, and statistics for the use of law enforcement agencies.

ORC Section 109.57 (C)(5) allows the attorney general to adopt rules under Chapter 119 of the ORC establishing guidelines for the operation of and participation in OHLEG, including criteria for granting and restricting access to information gathered and disseminated through OHLEG. These guidelines have been adopted and are codified in the OHLEG Rules and Regulations. The initial rules were adopted in April 2005, with updates on data security and use policy in June 2014. The rules for facial recognition were adopted in July 2016.

The following rules and regulations apply to criminal justice agencies (CJA) that wish to access OHLEG.

1.0 User Agreement

Any CJA that requests access to OHLEG must sign the OHLEG Agency/User Agreement. The signature of the agency chief executive officer also is required. The agency acknowledges that it is responsible for enforcing and adhering to all OHLEG Security Policies and agrees to accept responsibility for all users from that agency.

Each individual user must sign the OHLEG Agency/User Agreement. All users agree that access to OHLEG is limited to use for criminal justice purposes only.

1.1 Access restrictions

OHLEG law enforcement users are given access to a wider range of OHLEG attributes than are non-law enforcement users, such as court officials. The CEO of each agency is responsible for determining and enforcing access restrictions. Users are permitted to access only those OHLEG attributes that are directly related to their job responsibilities.

Access to individual attributes shall be based on the agency to which the user is assigned at the time of the use. OHLEG users who participate through multiple agencies shall log in to OHLEG using only the OHLEG Agency Identifier number for the agency for which they are working at the time of access. The CEO or designee determines the allowable attributes and should review those determinations when job assignments or responsibilities change. Any law enforcement officer who is a member of a task force may obtain a separate OHLEG account by contacting the OHLEG Support Center.

The nexus between an account holder's job assignment and OHLEG access is subject to review and validation during OHLEG Quality Assurance visits. These reviews are performed by Quality Assurance personnel from BCI, who essentially work as internal auditors. Users shall not attempt to access any data, documents, email correspondence or programs contained on OHLEG information resources for which they do not have authorization.

1.2 Access Control Criteria

Agencies should consider job assignments or functions of the user seeking access; physical location; network addresses; time of day and day of week/month restrictions when establishing rules for access to criminal justice information (CJI).

1.3 System Use Notification

OHLEG will display an approved system use notification message before granting access providing at a minimum the following information:

- The user is accessing a restricted information system.
- Unauthorized use of the system is prohibited and a violation of criminal law.
- System usage is subject to monitoring, recording and auditing.
- Use of the system indicates consent to monitoring and recording – the system includes all data, software, media and hardware.
- The law enforcement data maintained by BCI on the OHLEG site is provided at and subject to the discretion of BCI – BCI's grant of access to OHLEG confers upon the user no process or other rights in maintaining access.

The user must acknowledge the notification message before the user can gain access.

1.4 Personnel Security

Having proper security measures against inside threats is a critical component of the OHLEG security policies. This section's security terms and requirements apply to all personnel who have access to OHLEG, including those individuals with only physical or local access to devices that store, process or transmit unencrypted CJI. Access to OHLEG is a privilege and not a right.

The minimum screening requirements for individuals requiring access to CJI are as follows:

1. To verify identification, state of residence and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to OHLEG or CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to OHLEG.
2. The agency CEO shall specify the agency process for requesting OHLEG access.
3. If a felony conviction of any kind exists, the agency CEO shall deny access to OHLEG. However, the CEO may ask for a review by the OHLEG director in extenuating circumstances in which the severity of the offense and the length of time that has passed might support a variance.
4. If the person has a non-felony conviction or any arrest history without conviction, access to CJI shall not be granted until the agency CEO reviews the matter to determine whether access is appropriate.
5. If the person has an arrest history that includes any theft, domestic violence, menacing or stalking offense; telecommunications harassment; or any misuse of OHLEG, LEADS, or any other restricted law enforcement database or information, the CEO shall deny access. The CEO may ask for a review by the OHLEG director as indicated in #3 above.

6. If the person appears to be a fugitive, the person will be denied access to OHLEG.
7. If the person already has access to CJI and is subsequently arrested and/or convicted of a crime, access to OHLEG shall be terminated. If the crime is a non-felony, OHLEG access may be reinstated following a review by the agency CEO consistent with #4 and #5 above.
8. If the agency CEO, OAC or OHLEG director determines that access to OHLEG by an applicant/user would not be in the public interest, access shall be denied/removed. If access is denied/removed under this section, the agency shall notify the BCI/OHLEG Support Center in writing.
9. BCI/OHLEG's determination as to an OHLEG user's status is independent of, and unrelated to, his/her employment situation with his or her own agency. BCI will not make any determination about an OHLEG user's job status, a matter over which BCI exercises no authority or discretion.

1.5 OHLEG Access Procedure

No OHLEG user shall attempt to gain access to OHLEG or any OHLEG attribute beyond the specific access limits established and authorized by his or her employing agency.

- Requests for OHLEG access will be made via the OHLEG Online Account Application attribute, which is available on the homepage of any current OHLEG user.
- On each new user application, the Approver is required to certify that the basic training security video has been viewed by the applicant and that the OHLEG Agency/User Agreement has been signed by the user.
- The new applicant must physically enter his or her personal information in the appropriate sections on the online application.
- The Approver will select from a checklist the OHLEG attributes approved for each applicant.
- The Approver shall submit applications electronically to OHLEG administration for further processing and activation.
- The facial-recognition attribute will require specific authorization by the CEO of the agency and justification for each user indicating the investigative or other area of responsibility requiring such access.
- Non-law enforcement agencies generally will not have access to the facial-recognition attribute. Any non-law enforcement agency believing it has an exceptional need for access to the facial-recognition attribute may apply to the superintendent of BCI for facial-recognition access.

NOTE – No non-law enforcement agencies currently have, or have had, access to the facial-recognition attribute. A federal agency (which generally refers to law enforcement or criminal justice agencies) may be granted access if it has a presence in Ohio – for example, the FBI has offices in Columbus, Cleveland, Cincinnati and Dayton. On the state level, the BMV has investigators who are considered criminal justice agents.

At one time prior to the administration of Attorney General Yost, out-of-state agents and agencies had access to the facial-recognition database. An Aug. 14, 2014, article in The Cincinnati Enquirer indicates that about 150 users lost access after then-Attorney General Mike DeWine cut off access for out-of-state agencies. No out-of-state agencies currently have access.

Who has access to OHLEG?

The following types of law enforcement agencies have access to OHLEG, though not necessarily access to the facial-recognition attribute:

State

- Police departments
- Sheriff's offices
- Courts
- Parole authorities
- Prosecutors
- City attorneys
- State taxation authorities
- Department of Public Safety investigators
- Ohio State Highway Patrol
- Criminal task forces
- Drug enforcement agencies
- Department of Rehabilitation and Correction
- Ohio Pharmacy Board investigators
- Environmental Protection Agency
- Department of Natural Resources
- Ohio Lottery

Federal

- U.S. Department of Agriculture
- Air Force – Wright-Patterson Air Force Base
- Postal inspectors
- Department of Housing and Urban Development – Cleveland, Cincinnati, Akron
- U.S. Army – Columbus, Cleveland, Youngstown
- U.S. Marshals Service
- U.S. Immigration and Customs Enforcement
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- U.S. Border Patrol – Sandusky Bay
- Coast Guard – Lake Erie
- U.S. Secret Service
- U.S. Department of State
- Treasury Department – Cincinnati
- Department of Labor/Office of Inspector General – Cleveland
- U.S. Attorney's Office – Youngstown, Northern District, Southern District, Southern District of WV
- U.S. Customs – Cleveland
- U.S. Department of Defense Finance and Accounting
- U.S. Department of Education/Office of Inspector General
- Homeland Security
- U.S. Federal Protective Services
- U.S. Fish and Wildlife
- U.S. Forest Service
- Social Security Admin/Office of the Inspector General – Cleveland, Cincinnati

Maps from FreeVectorMaps.com

The scope of OHLEG data

OHLEG provides numerous applications and data sets for users:

- OHLEG Online Account Application
- OHLEG Roster (Only the CEO, Application approver or OHLEG Agency Coordinator (OAC) will have access to this application)
- Search Engine (SE) (This is where the facial-recognition attribute is located)
- Search Engine (SE) Admin (OHLEG helpdesk group only)
- Search Engine (SE) Lineup Wizard
- Record Management System
- eOPOTA Learning Management System (LMS) (A redirection to the OPOTA site)
- Missing Children's Clearinghouse
- Laboratory Evidence Pre-log and Inquiry
- Laboratory Online (Prosecutors only)
- OLLEISN Tackle (Ohio Local Law Enforcement Information Sharing Network/ Tracking All Crime Known to Law Enforcement, an information sharing network)
- OPOTA Online Registration and Certification
- Domestic Violence Reports
- Human Trafficking Reports
- Concealed-Carry Permit Statistics
- Pillbox Drug Identification
- Negative DNA Flag Offender Report
- Ohio Protection Order Registry 4.0
- RX Patrol (Provides a link to a nationwide searchable database of prescription-related thefts and related crimes. The database can be used to identify trends, support criminal cases and combat the abuse of prescription drugs.)
- School Safety Plans
- Blue Alerts, Amber Alerts and Missing Adult Alerts
- COLT (New application for sending letters to law enforcement agencies and prosecutors when the Bureau of Criminal Investigation has confirmed a DNA match.

Audits of OHLEG use

Quality assurance reviews of criminal justice agencies that use OHLEG are conducted every three years by Bureau of Criminal Investigation employees on the OHLEG Quality Assurance Audit Team. In 2018, 135 visits were made to agencies with access to OHLEG.

OHLEG is audited by the following agencies on a triennial cycle:

- National Sex Offender Registry (NSOR)
- Criminal Justice Information Services (CJIS) Security
- Law Enforcement Automated Data System (LEADS),
- National Data Exchange (NDEx)
- National Instant Criminal Background Check System (NICS)
- National Crime Information Center

The facial-recognition database is included in the regularly scheduled audits.

Five cases of OHLEG misuse have been documented in the past two years, but none involved the facial-recognition database. These cases are pending.

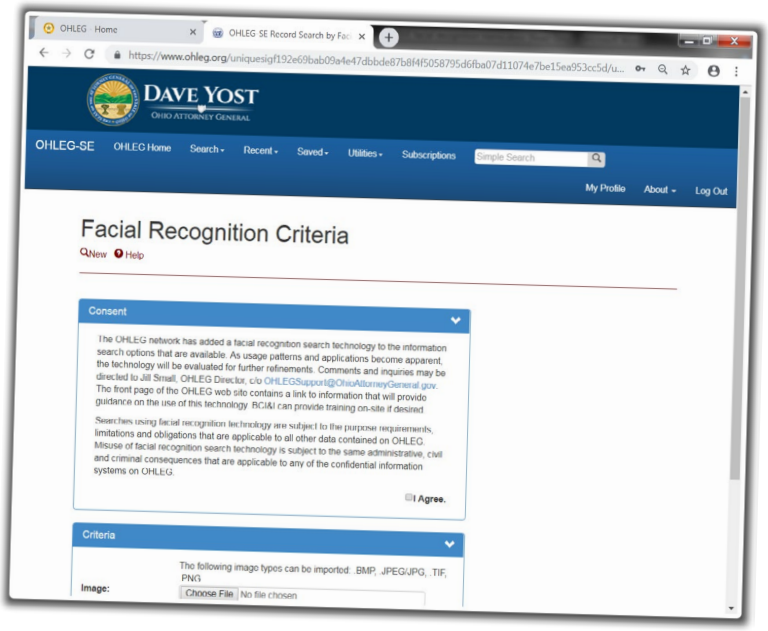
Currently, there are 52,680 OHLEG user accounts. However, 15,382 of these accounts have a status of *disabled* because the users have not logged in for 120 days. To regain access, these users would have to complete a new application. An additional 11,740 users are *suspended* because they have not logged in for 90 days. To regain access, they would have to contact OHLEG to reset their password. This leaves 25,558 active user accounts, 4,549 of which have facial-recognition access.

Process for law enforcement to access the facial-recognition system

Users of the facial-recognition database are subject to stringent access procedures and auditing practices.

To obtain access to the facial-recognition database:

- An agency must be confirmed to be eligible.
- The agency must be law enforcement (exceptions are permissible, but none has been made).
- The user must submit a new OHLEG application, and the application must be approved by the chief or sheriff of the agency (in limited cases, for very large agencies, there may be an additional facial-recognition approver designated by the chief or sheriff). After the information submitted by the chief or sheriff and the information on the new OHLEG application have been confirmed, the user can be activated for facial-recognition access.



Once the user is authorized to use the facial-recognition attribute, the mechanics for use are as follows:

- The user signs on to OHLEG using his/her personal sign-on information.
- A page appears with the attributes the user has permission to access.
- The user accesses the Search Engine attribute. Once on that page, if the user does not have permission to access facial recognition, it will not be an option on that site.
- When the user accesses the facial-recognition attribute, a consent/waiver appears and the user must agree to terms of use before being able to upload the search photo and launch the application. The consent form reinforces that facial-recognition searches are subject to the purpose requirements, limitations and obligations that are applicable to all other data contained on OHLEG.

- The law enforcement officer uploads the search photo and launches the facial-recognition program.
- The application returns photos, and identifiers, of persons matching certain algorithms within the facial-recognition system. The run returns anywhere from zero photos up to 20 photos, depending on the match. As with fingerprints, the better the sample, the greater the likelihood of a useful result.

All facial-recognition search photos submitted by the user and the photos in user-saved search results are stored in the OH-LEG-SE FacialRecognitionImage table with no retention limits. All image keys of facial-recognition search results are stored in the SearchResultFacialRecognition table whether or not the user saves the search results. This allows the user to view recent facial-recognition search results from the Recent Searches menu, even though they may not have saved those results. This also allows the Quality Assurance Audit Team to audit all facial-recognition searches.

Photos in the facial-recognition database

The facial-recognition database consists of photos from a variety of sources.

These photos were sent to a vendor and uploaded into the database. There are currently more than 24 million images in the facial-recognition database (24,380,731 as of July 2019). The sources of those photos include:

21,240,729: Ohio Bureau of Motor Vehicles

2,404,041: Ohio Supreme Court/Ohio Courts Network

276,816: Ohio Department of Rehabilitation and Correction

250,056: Columbus Division of Police

174,556: Hamilton County Sheriff's Office

31,351: Ohio Attorney General's Sex Offender Registry

2,173: Allen County Sheriff's Office

385: Hancock County Sheriff's Office/Findlay Police Department

332: Lima Police Department

292: Jefferson County Sheriff's Office/Steubenville Police Department

Bureau of Motor Vehicle photos

In August 2012, then-BCI Superintendent Thomas Stickrath and Director Thomas Charles, Ohio Department of Public Safety, Bureau of Motor Vehicles entered into a memorandum of understanding under which the BMV would provide information to the AGO and BCI and the BMV could avail itself of the AGO's facial-recognition system and/or receive facial-recognition analytical information from the AGO. The BMV agreed to provide Ohio vehicle registration and driving record information, digitized photographic records of Ohio DL/IDs and other Ohio operator's license information, including demographic information, license number and license status.

The BMV also agreed to transfer to the AGO $208,500 toward the AGO's development of the facial-recognition system. The AGO agreed to provide the BMV full use of the AGO's facial-recognition system except where use is limited by federal or state law.

The MOU was extended through the years with the most recent extension, Tenth Amendment To and Renewal of the MOU, executed in December 2018 and effective Jan. 1, 2019, through December 2019.

Initially, BMV investigators were using facial recognition to determine if those applying for or renewing an Ohio driver's license were who they said they were. The investigators were able to identify 26 people submitting false identifications between the short time that the facial-recognition program was launched and the temporary suspension of the program by then-Attorney General Mike DeWine for a system review.

Between August and December of 2012, the BMV provided all driver's license ID photos from 2011 and earlier to OHLEG for the facial-recognition database. The BMV has provided no further photos to OHLEG, so all facial-recognition runs are utilizing BMV photos from 2011 and earlier.

State, federal laws governing the use of photos from the Ohio BMV

Ohio Revised Code Section 109.57 sets forth the duties of the superintendent of Bureau of Criminal Investigation. Of note are duties listed in (A)(3) mandating that the superintendent assist sheriffs, chiefs of police and other law enforcement officers in establishing a complete system of criminal identification and in obtaining fingerprints and other means of identification of all persons arrested on a felony charge (and other crimes).

Section (C)(1) authorizes the superintendent to operate a center for electronic, automated or other data for the processing for the storage and retrieval of information, data and statistics pertaining to criminals and delinquents. The superintendent may also establish and operate a statewide communications network (the Ohio Law Enforcement Gateway) to gather and disseminate information, data and statistics for the use of law enforcement agencies and for other uses specified in this division. Section (C)(3) allows the superintendent or his designee to provide and exchange the information, data and statistics pursuant to the national crime prevention and privacy compact.

ORC 109.57(C)(5) allows the Ohio attorney general to adopt rules pursuant to Chapter 119 establishing guides for the operation of and participation in OHLEG.

Pursuant to **109.57(D)(4)**, data and statistics gathered or disseminated through OHLEG and other information that is set forth in sections (F) and (G) are not public records.

Although **ORC 4501.27(A)** prohibits the knowing disclosure, or making available, to any person or entity any personal information about an individual that the Ohio BMV obtains in connection with a motor vehicle record, **Section 4501.27(B)(2)** allows for the bureau to disclose such information to a government agency, including a court or law enforcement agency, in carrying out its functions or for the use of a private person or entity acting on behalf of an agency of this state, another state, the United States, or a political subdivision of Ohio or another state in carrying out its function.

Title 18 USC Section 2721 prohibits the release of certain personal information from state motor vehicle records except when there is a permissible use. A permissible use is defined in Subsection (b) and allows for the release in connection with matters of motor vehicle or driver safety and theft. Subsection (b)(1) also allows release of the information for use by any government agency, including any court or law enforcement agency in carrying out its function.

While both the federal and state statutes place limitations on the release of personal information from BMV records, they both permit the release of personal information from motor vehicle records to courts and law enforcement agencies carrying out their functions.

The proposed memorandum of understanding between BCI, FBI

In August 2017, the FBI and then-BCI Superintendent Thomas Stickrath contemplated entering into an MOU concerning the FBI's use of Ohio's facial-recognition database. This MOU was never executed. It is unclear why the MOU was not executed.

It is worth noting that the proposed MOU would not have given the FBI any elevated access to the database. Essentially, the MOU was intended to ensure that OHLEG's handling of FBI facial-recognition searches was being conducted in compliance with federal regulations governing the confidentiality and use of criminal justice information. However, OHLEG's procedures already are compliant with federal law, making the MOU unnecessary.

Agents from the FBI already were authorized to access the facial-recognition attribute if they were located in Ohio, were authorized to access OHLEG, were approved by the highest ranking agent of their office to access the facial-recognition attribute, approved for access to the facial-recognition attribute and had an active criminal case.

The intent of the proposed MOU was to add layers of protection for the individuals whose pictures were in the database when the facial-recognition attribute was used. The FBI was physically examining the returned photos in an effort to identify only likely candidates. Had BCI and the FBI executed the MOU, the step-by-step process for an FBI special agent to access the database would have been as follows:

- The special agent would send the search photo to the FBI Criminal Justice Information Services Division, or CJIS, in Clarksburg, West Virginia.
- After review by agents at CJIS, the photo would be sent to BCI's Criminal Intelligence Unit (CIU). CIU analysts would upload the photo and run the facial-recognition program. Any results from the search would be sent to agents with the Criminal Justice Information Services Division, who would manually analyze, compare and evaluate the candidate photo gallery against the search photo to determine the most likely candidate.
- The FBI would use the most likely candidate photo in a search of the FBI's Next Generation Identification Interstate Photo System. The results of this search would be compared with and analyzed against the original search photos.
- Once this analysis was completed, the most likely candidate photo would be provided to the requesting FBI personnel as an investigative lead.

Images and information associated with any most likely candidate(s) would be stored in the FBI Case Management System for record keeping, and the other photos and information not associated with a most likely candidate would be destroyed.

DAVE YOST
OHIO ATTORNEY GENERAL

Facial-Recognition Inquiries

For more information about this report, please contact:

Ohio Attorney General's Office
30 E. Broad St., 17th Floor
Columbus, OH 43215

614-466-3840

www.OhioAttorneyGeneral.gov