House Bill 1245

By: Representatives Cummings of the 39th, Smith of the 18th, Vance of the 133rd, Crowe of the 118th, and Neal of the 79th

A BILL TO BE ENTITLED

AN ACT

To amend Chapter 1 of Title 35 of the Official Code of Georgia Annotated, relating to general provisions regarding law enforcement officers and agencies, so as to provide for definitions; to provide for legislative intent and findings; to provide for the use and limitations of use of facial recognition technology by law enforcement agencies in this state; to provide for procedures for the use of such software; to provide for certain prohibitions; to provide for requests for assistance to other law enforcement agencies; to provide for certain releases and indemnities with regard to such requests for assistance; to provide for certain auditing; to provide for violations and penalties; to provide for related matters; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Chapter 1 of Title 35 of the Official Code of Georgia Annotated, relating to general provisions regarding law enforcement officers and agencies, is amended by adding a new Code section to read as follows:

"35-1-24.

(a) As used in this Code section, the term:

(1) 'Candidate list' means one or more facial images from a facial recognition search using facial recognition software.

(2) 'Facial recognition repository' means a location or data base, digital or otherwise, in which facial images are collected and stored for comparison during a facial recognition search.

(3) 'Facial recognition search' means an automated process of matching facial images utilizing algorithms and biometric scanning technologies.

(4) 'Facial recognition software' means computer programs that use algorithms and biometric scanning technologies to compare and match facial images with a probe image.

(5) 'Facial recognition specialist' means a person trained and authorized to use facial recognition software and whose duty it is to conduct facial recognition searches.

(6) 'Likely candidate' means a specific image contained within a candidate list depicting the face of a person which, when combined with a human-based facial comparison, depicts sufficient similarities or attributes to warrant further investigation and peer review.

(7) 'Peer review' means an additional layer of verification of facial recognition results by which another facial recognition specialist conducts an independent probe image search using a blind review.

(8) 'Probe image' means any facial image used by facial recognition software for comparison with the facial images contained in the facial recognition repository or repositories used by the facial recognition software.

(b)(1) It is the policy of the State of Georgia that facial recognition software be used by law enforcement agencies only for the purposes of identifying persons involved in criminal cases, other special law enforcement related purposes, and in the support of public welfare.

(2) The State of Georgia continually seeks to balance the use of technology-based investigative tools against privacy concerns to ensure that the constitutional rights and the safety of all individuals are both protected.

(3) Facial recognition software is intended to assist law enforcement officers and agencies with identifying criminal actors while ensuring that improper or incorrect visual identification does not lead to the arrest or prosecution of an innocent individual. It is intended to provide investigators with tools to develop possible suspects in crimes based upon similarities in facial characteristics.

(4) Facial recognition searches may be used as an item of evidence in a criminal investigation. However, it is the obligation of the law enforcement officer and agency to ensure that the necessary level of additional supporting evidence exists to establish needed legal standards to pursue criminal charges. Facial recognition searches may also be used by law enforcement officers and agencies to support public welfare and medical related events to assist with the identification of individuals.

(c) Law enforcement officers in criminal cases shall seek corroborating evidence on any person identified after receiving the results of a facial recognition search of a probe image on facial recognition software authorized by the agency employing the law enforcement officer. Such corroborating evidence should independently support probable cause for criminal charges. Law enforcement officers who are authorized to use facial recognition data bases shall only do so through a facial recognition specialist authorized to perform such facial recognition searches by the agency by which the law enforcement officer is employed and shall use only lawfully acquired facial images for use as probe images and shall use only agency-authorized facial recognition repositories containing lawfully acquired facial images and publicly available image galleries.

(d) Uses for which law enforcement officers and agencies may conduct facial recognition searches are to assist in:

(1) Identifying an individual when there is a reasonable suspicion that the individual has committed, is committing, or is planning the commission of a crime;

(2) Identifying a crime victim, including a victim of online sexual abuse material;

(3) Identifying a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or wildlife;

(4) Identifying a person that may be a missing person;

(5) Identifying a person who is suffering from an inability to communicate and be understood as the result of an apparent mental or physical disability;

(6) Identifying a deceased person;

(7) Identifying a person who is incapacitated or otherwise unable to identify himself or herself;

(8) Identifying an individual who is lawfully detained; and

(9) Mitigating an imminent threat to public safety or a significant threat to life, including acts of terrorism.

Any result from a facial recognition search shall be used only as a guide for further investigation.

(e) Each law enforcement agency desiring to utilize facial recognition software and do facial recognition searches shall first adopt in writing the use of such facial recognition software and establish standard operating procedures for the agency in the use of such software.

(f) The standard operating procedure for use of facial recognition software and searches shall include procedures that cover the following requirements:

(1) A law enforcement agency shall prior to authorizing the use of facial recognition software ensure that the facial recognition specialist who will operate the facial recognition software has satisfactorily completed agency approved training in the use of such software; shall assign each such facial recognition specialist a unique username and

password for the use of such facial recognition software; and shall ensure that only authorized persons use such facial recognition software;

(2) When using facial recognition software, the facial recognition specialist shall:

(A) Use the facial recognition software only for official and legitimate law enforcement business;

(B) Log in using the username and password assigned such specialist;

(C) Record the case number in the incident report and, if applicable, in the investigative data base;

(D) Record the legitimate law enforcement reason or basis for the search in the incident report and, if applicable, in the investigative data base;

(E) Only utilize probe images that have been collected in accordance with state and federal law;

(F) Only use facial recognition software that is approved and authorized by the law enforcement agency; and

(G) Ensure that each member of the law enforcement agency who submits a request for a facial recognition search correctly documents such request and the results of such search, whether such search results in any investigative leads or not, in the incident report; and

(3) All facial recognition searches to attempt to identify an unidentified suspect in a criminal investigation shall be performed in the following sequence and manner:

(A) A facial recognition search shall be performed by a facial recognition specialist using a probe image of the unidentified suspect utilizing a facial recognition repository and facial recognition software approved by the law enforcement agency;

(B) Following a facial recognition search which yields a candidate list of likely candidates, a human-based facial comparison shall be made of the persons in the candidate list;

(C) In addition, a peer review of the likely candidates on the candidate list shall be made;

(D) Following the human-based facial comparison and peer review of the candidates on the candidate list, investigations shall be made of the likely candidates to reveal corroborating or exculpatory evidence;

(E) Prior to pursuing criminal charges or warrants in a matter under investigation in which a facial recognition search was made, a superior officer shall review the case to ensure that procedures were followed and there is sufficient evidence to seek warrants for the suspect; and

(F) The evidence shall be submitted to the proper judge for review prior to the issuance of any warrants.

(g) No person on behalf of a law enforcement agency or law enforcement officer in this state shall connect any facial recognition software to any interface that performs live video surveillance, including, but not limited to, surveillance cameras, drone cameras, and body-worn cameras. This subsection shall not however preclude the use of still images or snapshots from being captured from video streams and used as probe images for a facial recognition search.

(h) No facial recognition software shall be utilized by or on behalf of any law enforcement agency or law enforcement officer on live stream or recorded video of the general public or for surveillance of the general public.

(i) The use of force to capture a person's image for a probe image in a facial recognition search shall be illegal.

(j) Only facial recognition software that is approved by the law enforcement agency in writing shall be used for facial recognition searches. It shall be illegal for law enforcement agencies and law enforcement officers to use facial recognition software that is obtained through a complimentary pilot program, demonstration program, personal account, or trial period in any law enforcement investigation.

(k) Access to the facial recognition software of a law enforcement agency by another law enforcement agency shall require a written request for assistance from a supervisory level official of the requesting law enforcement agency which shall be reviewed and approved by a supervisory level official of the law enforcement agency to which the request is made. The requesting law enforcement agency shall submit with the request for access to facial recognition services a signed interagency agreement or memorandum of understanding which acknowledges that:

(1) The requesting law enforcement agency agrees to comply with all provisions of law regarding the conduct and use of facial recognition software and searches;

(2) The requesting law enforcement agency acknowledges that the results from a facial recognition search shall not be considered as a positive identification of any person;

(3) The requesting law enforcement agency will use the facial recognition software and searches for legitimate law enforcement purposes only which shall be limited to the identification of suspects in criminal investigations, the identification of persons unable to identify themselves, and other purposes specifically authorized by the law enforcement agency to which the request is made;

(4) Facial recognition software shall not be used for surveillance or tracking purposes;

(5) The requesting law enforcement agency shall not utilize the results of a facial recognition search alone for the purpose of establishing an articulable suspicion for an investigatory stop of an individual, probable cause for an arrest, or probable cause for a search warrant. The requesting agency shall pursue criminal charges against an individual identified by a facial recognition search only when there is corroborating evidence creating probable cause to believe that such individual committed a crime;

(6) The requesting law enforcement agency shall use facial recognition software in accordance with federal and state statutory and constitutional law and in accordance with the requirements and procedures of the agency to which the request is made;

(7) The results and any other information obtained as a result of a facial recognition search will be kept confidential except as disclosure is otherwise permitted by law and will be held and purged in accordance with the retention policy of the requesting agency; and

(8) The probe images which are submitted by the requesting law enforcement agency were lawfully obtained and do not violate the privacy rights, publicity rights, copyrights, contract rights, intellectual property rights, or any other rights of any person and that the use of the probe images in conjunction with a facial recognition search using the facial recognition software of the law enforcement agency to which the request is made will not result in a breach of contract between the requesting law enforcement agency and any third party.

(l) A law enforcement agency which requests access to the facial recognition software of another law enforcement agency which request is granted shall be deemed to have released the governing authority of the law enforcement agency to which the request is made, the members of the governing authority, the governmental entity, the law enforcement agency to which the request is made, and all officers, elected officials, employees, agents, volunteers, and representatives of such governmental entity and law enforcement agency, both in their individual and representative capacities, from any responsibility or liability for any actions, causes of actions, claims, demands, costs, liabilities, expenses, or damages which are in any way connected to the information provided by the law enforcement agency to which the request for use of facial recognition software was made or any loss or damage arising from, or allegedly arising from, the information provided by the law enforcement agency to which the request for use of facial recognition software was made. This release shall not apply to any claims arising from intentional misconduct on the part of the law enforcement agency or any of its personnel to which the request for use of facial recognition software is made.

(m) By requesting access to the facial recognition software of another law enforcement agency, the requesting law enforcement agency shall be deemed to have agreed to defend and hold harmless the law enforcement agency to which the request was made, the governing authority of the law enforcement agency to which the request is made, the members of the governing authority, the governmental entity, and all officers, elected officials, employees, agents, volunteers, and representatives, both in their individual and representative capacities, from any and all claims and liability for damages, property damages, and personal injuries or damages, including death, judgments, causes of action, liens, costs, and legal expenses, including attorney fees, in any way connected to or stemming from the information provided by the law enforcement agency to which the request was made for a facial recognition search to the requesting agency. In addition, the requesting law enforcement agency shall also indemnify and hold harmless the law enforcement agency to which the request for a facial recognition search was made and the other parties identified in this subsection from and against all claims, actions, suits, proceedings, losses, damages, costs, and expenses, including attorney fees, arising out of or resulting from, directly or indirectly, any failure of the requesting agency to comply with the provisions of this Code section and the interagency agreement or memorandum of understanding regarding the use of facial recognition software or the conduct of facial recognition searches pursuant to such agreement or memorandum.

(n) Any law enforcement agency utilizing facial recognition software shall maintain and ensure compliance with the provisions of this Code section and state and federal law with regard to the use of such software. As a part of such program to ensure compliance, the law enforcement agency shall conduct random sample audits of authorized users of such facial recognition software on a quarterly basis. Such audits shall, at a minimum, review whether the proper documentation is being created and maintained regarding the use of the facial recognition software, including the case number, the reason for the facial recognition search, the name of the law enforcement officer or officers for whom the search was

performed, the unit to which such officer or officers are assigned, and any other information required to be obtained and maintained under the policy of the law enforcement agency. In addition, at least annually, the law enforcement agency shall perform a random sample audit to verify that the proper procedures for conducting facial recognition searches and all investigative steps are being followed and that the list of authorized users of the facial recognition software is current and that all users who no longer need access to the software have been removed. All such audits shall be documented and maintained by the agency for a period of at least two calendar years.

(o) Any person who intentionally misuses facial recognition software shall be guilty of a misdemeanor.

(p) Each law enforcement agency which uses facial recognition software shall establish policies under which the ability of users of such software shall be suspended or revoked if such users are found to have failed to comply with this Code section or other applicable state and federal laws regarding the use of facial recognition software."

SECTION 2.

All laws and parts of laws in conflict with this Act are repealed.