WEST VIRGINIA LEGISLATURE

2025 REGULAR SESSION

Introduced

Senate Bill 688

By Senators Rose, Thorne, Rucker, and Willis

[Introduced March 4, 2025; referred

to the Committee on Government Organization; and

then to the Committee on the Judiciary]

A BILL to amend the Code of West Virginia, 1931, as amended, by adding a new article, designated §15-17-1, §15-17-2, §15-17-3, §15-17-4, §15-17-5, and §15-17-6, relating to prohibiting law-enforcement officers and political subdivision officials from irresponsibly utilizing certain surveillance technologies and artificial intelligence facial recognition technologies; setting forth legislative findings; providing definitions; and establishing parameters for the responsible and constitutional use of these technologies.

Be it enacted by the Legislature of West Virginia:

ARTICLE 17. RESPONSIBLE USE OF FACIAL RECOGNITION ACT.

§15-17-1. Short Title.

This article shall be known as the "Responsible Use of Facial Recognition Act."

§15-17-2. Legislative Findings.

The Legislature hereby finds and declares that the Fourth Amendment to the Constitution of the United States of America provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrant shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Legislature further finds that Article 3-5 of the Constitution of the State of West Virginia provides that "The rights of citizens of this state to be secure in their houses, persons, papers and effects, against unreasonable searches and seizures, shall not be violated. No warrant shall issue except upon probable cause, supported by oath or affirmation, particularly describing the place to be searched, or the person or thing to be searched." The Legislature finds further that innovations in surveillance and artificial intelligence pose unique threats to the constitutional protections against unreasonable searches and seizures. The Legislature additionally finds that these innovations in surveillance and artificial intelligence recognition technology constitute a powerful tool that can be used to combat serious and organized crime, prevent fraud, identify victims, and protect citizens of West Virginia. The Legislature additionally recognizes that appropriate limitations and guardrails are required to ensure that government actors do not misuse facial recognition technology, including in any manner that would pose a threat to the constitutional protections against unreasonable searches and seizures. Therefore, the Legislature finds and declares that law enforcement's use of facial recognitions technological innovations in surveillance and the use of artificial intelligence int facial recognitions must be closely regulated in accordance with the provisions set forth in this article and subject to publicly available use policies that are developed in accordance with this article.

The Legislature further finds and declares that foreign adversarial nations are actively engaged in seeking to harm the national security of the United States of America and the interests of the citizens of West Virginia, and that the foreign technology providers may utilize sub-contractors, employees, and agents from foreign adversarial countries to develop core technology. The Legislature finds that foreign technology providers in surveillance and artificial intelligence have frequently been coopted by foreign adversary governments; that surveillance and artificial intelligence facial recognition technology has the potential to access sensitive government data and investigative records, which, if accessed by foreign adversaries through an intentional security breach, would cause irreparable harm. The Legislature further finds that surveillance and artificial intelligence facial recognition technology may be used to implant back door system access or create security vulnerabilities in critical law enforcement systems. As such, the Legislature finds that foreign adversarial technology providers in facial recognition technology pose an immediate and material threat to the data security of the citizens of West Virginia, as well as to the national security of the United States of America. Therefore, the Legislature finds and declares that law enforcement's use of surveillance and artificial intelligence facial recognition technology must utilize American-developed technologies that are exclusively developed and manufactured in the United States.

§15-17-3. Definitions.

As used in this article:

(1) "Facial recognition technology" means the use of algorithmic comparison of images of individual's facial features for the purposes of verification or identification, unless used for the sole purpose of authentication in order to access a secure device or secure premises;

(2) "Law enforcement agency" means any public agency that employs a law enforcement officer as defined in §30-29-1 and the West Virginia Division of Motor Vehicles, acting directly or through its duly authorized officers and agents, as defined in West Virginia Code §17A-1-1, *et seq.*; and

(3) "Model facial recognition technology policy" means the model policy developed and published under this article regarding the use of facial recognition technology.

§15-17-4. Prohibition against unreasonable surveillance and artificial intelligence technologies.

Use of the following technologies by law enforcement constitutes unreasonable searches and may not be used by any law enforcement officer or any person for law enforcement purposes unless a warrant has been issued authorizing such use against a specific person based upon probable cause:

(1) Real Time Security monitoring;

(2) Multimodal vehicle recognition;

(3) Facial recognition;

(4) Surveillance drones;

(5) License plate readers; and

(6) Digital identity ecosystems.

§15-17-5. Facial recognition working group and use policies.

(a) A working group on facial recognition technology is hereby created and shall be attached to the West Virginia Department of Homeland Security for administrative purposed. The working group shall be chaired by the secretary of the West Virginia Department of Homeland Security or his or her designee and composed of representatives from the following organizations as nominated by the secretary as nominated and appointed by the Governor:

(1) The West Virginia Chiefs of Police Association;

(2) The West Virginia Sheriff's Association;

(3) The West Virginia State Police;

(4) The West Virginia Association of Counties; and

(5) The West Virginia Law Enforcement Professional Standards (LEPS) Subcommittee of the Governor's Committee on Crime, Delinquency and Corrections.

(b) On or before January 1, 2026, the working group established pursuant to §15-17-5(a) of this code shall create and make publicly available a model policy for use by law enforcement agencies, which shall:

(1) Specify the authorized uses of facial recognitions technology consistent with the law, including but not limited to:

(A) How search results using facial recognition technology relate to establishing probable cause for arrests; and

(B) The prohibition of using facial recognition technology to identify a person participating in constitutionally protected activities in public spaces unless there is probable cause to believe that a criminal offense has been committed;

(2) Specify requirements for persons within a law enforcement agency that are authorized to use facial recognition technology;

(3) Require a law enforcement agency to specify a process for the agency to document instances in which facial recognition technology is used;

(4) Provide procedures for the confirmation of any initial findings generated by facial recognition technology by human personnel trained in facial examination procedures and processes developed in accordance with the provisions of subsection (7) of this section;

(5) Specify data integrity and retention policies applicable to the data collected with a warrant by the law enforcement organization, including processes that address:

(A) Maintenance and updating of records used;

(B) A routine audit schedule to ensure compliance with the policy;

(C) The length of time the organization will keep the data; and

(D) The processes by which the data will be deleted;

(6) Specify data security measures applicable to the law enforcement agency's use of facial recognition technology; including:

(A) How data collected will be securely stored and accessed; and

(B) Rules and procedures for sharing data with other entities, which ensure that those entities comply with the sharing agency's policy as part of the data-sharing agreement;

(7) Specify training procedures and processes to endure all personnel who utilize facial recognition technology or access its data are knowledgeable about and able to ensure compliance with the policy;

(8) Specify a process that requires a law enforcement agency utilizing facial recognition technology to compare a publicly available or lawfully acquired image against a database of publicly available or lawfully acquired images;

(9) Specify a minimum accuracy standard for face matches with reference to the Face Recognition Technology Evaluation (FRTE) conducted by the National Institute of Standards and Technology (NIST);

(10) Provide a specific mechanism to produce a record of prior uses of facial recognition technology that can be used to audit and verify images and information used to make a match of a person; and

(11) Provide a process that addresses the privacy of persons by excluding, redacting, blurring, or otherwise obscuring nudity or sexual conduct involving any identifiable person.

(c) A law enforcement agency that uses facial recognition technology shall have a use policy in place prior to using the technology. A law enforcement agency shall file a full copy of its policy or any revision of its policy with the West Virginia Department of Homeland Security within

30 days of the adoption or revision.

(d) This section shall not apply to generally available consumer product that includes facial recognition technology, provided that the facial recognition technology is intended only for personal or household use. This section applies to use of facial recognition technology by the public sector and not to commercial use of facial recognition technology.

§15-17-6. Minimum standards.

(a) West Virginia law enforcement agencies and political subdivisions must only procure or use facial recognition technology that is entirely produced in the United States by an American company headquartered in the United States and is not owned or controlled by a company that is based outside the United States,

(b) Any facial recognition algorithm used by a law enforcement agency must be subjected to both NIST FRTE 1:1 and NIST FRTE 1:N testing and must demonstrate high accuracy and performance in such NIST testing;

(c) Facial recognition technology should never be used to suppress civil liberties or rights recognized under the Constitution of the United States of America or civil liberties of rights recognized under the Constitution of West Virginia;

(d) Facial recognition technology should not be used to establish the sole support of probable cause for an arrest, search, or seizure of any West Virginia citizen or any property. Independent evidence must be required to establish probable cause;

(e) Facial recognition technology use must be in compliance with public authority and/or law enforcement policies and procedures, all ordinances, statutes, and regulations, applicable court orders, and supervisory frameworks, and all limits of the Constitution of the United States of America and the Constitution of West Virginia that protect civil liberties, individual freedoms, and citizen rights; and

(f) Facial recognition technology use by law enforcement agencies may only be utilized with images that are legally collected by law enforcement or other government agencies and not by private entities in violation of law using methods that are prohibited for public entities. Investigative records and images used by facial recognition technology may not be provided to private entities but must remain at all times within public systems.

NOTE: The purpose of this bill is to require law enforcement officers and political subdivision officials from irresponsibly utilizing certain surveillance technologies and artificial intelligence facial recognition technologies, setting forth legislative findings, providing definitions, establishing parameters for the responsible and constitutional use of these technologies.

Strike-throughs indicate language that would be stricken from a heading or the present law and underscoring indicates new language that would be added.