H-2022.1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SUBSTITUTE HOUSE BILL 1654**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**State of Washington 66th Legislature 2019 Regular Session**

**By** House Innovation, Technology & Economic Development (originally sponsored by Representatives Ryu, Shea, Morris, Valdez, Kloba, Fitzgibbon, Appleton, Frame, and Tarleton)

 AN ACT Relating to the procurement and use of facial recognition technology by government entities in Washington state and privacy rights relating to facial recognition technology; and adding a new chapter to Title 10 RCW.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec.**  FINDINGS. The legislature finds that:

(1) Washingtonians cherish privacy as an essential element of their individual freedom, and Washington explicitly recognizes its citizens' right to privacy in its Constitution under Article I, section 7.

(2) Facial recognition technology poses unique and significant civil rights and civil liberties concerns.

(3) Studies have found facial recognition technology to be less accurate at identifying women, youth, and people of color, leading to the risk of false matches.

(4) There is a long history of the use of previous surveillance technologies to impact vulnerable communities, such as the use of social media monitoring systems to track black lives matter activists and license plate readers to track Muslim community members, and the government of China is currently using facial recognition and other technologies for general monitoring and social control.

(5) The use of facial recognition technology without warrant or suspicion can chill the exercise of constitutionally protected free speech, assembly, religious, privacy, and other rights.

(6) Before the widespread adoption of facial recognition technology by government agencies occurs, there must be a public discussion of acceptable uses of this technology, its accuracy must be demonstrated, and disproportionate impacts on vulnerable communities eliminated.

NEW SECTION. **Sec.**  DEFINITIONS. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Facial recognition" means both:

(a) The automated or semiautomated process by which a person is identified or attempted to be identified based on the characteristics of their face, including identification of known or unknown individuals or groups; and

(b) The automated or semiautomated process by which the characteristics of an individual's face are analyzed to determine the individual's sentiment, state of mind, or other propensities including but not limited to level of dangerousness.

(2) "Facial recognition system" means any computer software or application that performs facial recognition.

NEW SECTION. **Sec.**  GOVERNMENT USE OF FACIAL RECOGNITION SYSTEMS. (1) Until the conditions set forth in subsection (2) of this section are met, all government entities must follow the procurement practices in chapter 40.26 RCW in order to obtain, retain, access, or use:

(a) Any facial recognition system; or

(b) Any information obtained from or by use of a facial recognition system.

(2) The restrictions set forth in subsection (1) of this section remain in effect until such time as:

(a) The attorney general provides a report certifying to the legislature that:

(i) Independent, third-party testing and auditing of the accuracy of the five most commonly available facial recognition systems by market share, under operational conditions, has taken place; and

(ii) Such testing and auditing shows no statistically significant variation in the accuracy of such systems on the basis of the race, skin tone, ethnicity, gender, or age of the individuals portrayed in probe images, whether or not those categories are applied individually or in combination;

(b) The Washington academy of sciences convenes a task force and the task force delivers to the legislature a report documenting the potential consequences and the best procurement practices of government use of facial recognition systems on the civil rights and civil liberties of all Washingtonians, including vulnerable communities. The task force must consist of fifteen members who represent: (i) Communities historically impacted by surveillance technologies, including, but not limited to, African American, Hispanic American, Native American, and Asian American communities, religious minorities, protest and activist groups, and other vulnerable communities; (ii) organizations that advocate for data privacy protections for the public at large; and (iii) different branches of law enforcement, facial recognition technology vendors, and appropriate academic experts; and

(c) On the basis of the reports set forth in (a) and (b) of this subsection, the legislature passes legislation finding that the conditions set forth in this subsection (2) have been met, and includes appropriate, recommended restrictions on facial recognition systems' use by government agencies.

NEW SECTION. **Sec.**  PRIVACY RIGHTS RELATING TO FACIAL RECOGNITION TECHNOLOGY. (1) This section applies to all Washington state and local government agencies.

(2) It is unlawful for any state or local government agency or state or local government official to monitor public spaces without a probable cause using any facial recognition system or data obtained therefrom; or to use facial recognition to analyze, whether or not contemporaneously, any footage obtained from a police body worn camera.

NEW SECTION. **Sec.**  ENFORCEMENT. (1) No data collected or derived from any use of facial recognition in violation of this chapter and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority subject to the jurisdiction of the state of Washington. Facial recognition data collected or derived in violation of this chapter must be considered unlawfully obtained and must be deleted upon discovery.

(2) Any violation of this chapter constitutes an injury and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in any court of competent jurisdiction to enforce this chapter. An action instituted under this subsection may be brought against the appropriate state or local government agency or state or local government official and, if necessary to effectuate compliance with this chapter, any other government agency with possession, custody, or control of data subject to this chapter.

(3) Any person who has been subjected to facial recognition in violation of this chapter, or about whom information has been obtained, retained, accessed, or used in violation of this chapter, may institute proceedings in any court of competent jurisdiction against the state and is entitled to recover actual damages, but not less than liquidated damages of one thousand dollars or one hundred dollars for each violation, whichever is greater.

(4) A court shall award costs and reasonable attorneys' fees to a plaintiff who is the prevailing party in an action brought under subsection (2) or (3) of this section.

NEW SECTION. **Sec.**  Sections 1 through 5 of this act constitute a new chapter in Title 10 RCW.

**--- END ---**