A BILL FOR AN ACT

RELATING TO FACE SURVEILLANCE.

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

SECTION 1. The legislature finds that the unregulated use of face surveillance poses a unique and significant threat to the civil rights and liberties of residents and visitors of Hawaii, especially with regard to the rights guaranteed by the First, Fourth, and Fourteenth Amendments of the Constitution of the United States and article I, sections 4, 5, 6, and 7 of the Hawaii State Constitution.

The legislature further finds that a study published in 2019 by the National Institute of Standards and Technology found that the majority of face surveillance technology systems are far less accurate in identifying the faces of women, elderly people, children, and people of color. These inaccuracies place certain persons at an elevated risk of harmful "false positive" identifications. Multiple studies and a growing base of experts have had similar findings. Additionally, numerous studies have shown that many of the databases to which face surveillance
technology is applied are plagued by racial and other biases, which generate copycat biases in face surveillance data.

The legislature also finds that the broad application of face surveillance in public spaces is the functional equivalent of requiring every person to carry and display a personal photo identification card at all times and carry a government global positioning system tracking device, which constitutes an unacceptable mass violation of privacy without probable cause.

The legislature further believes that the benefits of using unregulated face surveillance can be outweighed by its harms.

One known advantage of face surveillance in Hawaii is that some county police departments have used face surveillance technology in a limited capacity, in coordination with the Hawaii criminal justice data center in the department of the attorney general.

In the police departments, surveillance images of a crime are compared against mugshots already existing in the Hawaii criminal justice data center's database. The face surveillance program is intended to identify possible suspects by generating investigative leads for detectives. While the face surveillance program is relatively new and has been used relatively few times, the results of the program have been promising. The
legislature believes that county police departments should be allowed to continue to use face surveillance for this limited purpose. However, until the technology matures and proper protections are put in place, the legislature finds further uses of face recognition technology should be vetted and approved by the legislature.

The legislature further finds that the increasing prevalence and sophistication of face surveillance technology for commercial purposes poses a unique threat to the civil rights and liberties of the State's residents and visitors. Commercial venues are beginning to incorporate face surveillance technology to support in-store tracking of individuals. The technology identifies individuals entering stores or, if the precise identity of an individual is yet unknown, surveys the individual's face to determine the individual's age and gender.

The legislature finds that this information is being sold to third parties or provided to foreign governments for purposes that are wholly inconsistent with the State's public policy and democratic principles. At least one foreign government is said to already have complete facial recognition profiles on all its citizens, which it uses to suppress free speech and invade the
privacy of people within its borders without restraint.

Hawaii's citizens should not be subject to such violation of privacy.

The purpose of this Act is to place a moratorium on:

(1) Government use of face surveillance other than existing police department use; and

(2) Private use of face surveillance unless the subject of the face surveillance has given clear, discrete, written consent,

to ensure the legislature can properly vet future uses of the rapidly evolving technology and prevent unintended consequences from befalling Hawaii residents and their privacy and freedom.

SECTION 2. The Hawaii Revised Statutes is amended by adding a new chapter to be appropriately designated and to read as follows:

"CHAPTER

FACE SURVEILLANCE

§ -1 Definitions. As used in this chapter:

"Face surveillance" means an automated or semiautomated process that:
(1) Assists in identifying or verifying an individual or capturing information about an individual based on the physical characteristics of the individual's face; or

(2) Uses characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of the individual.

"Face surveillance system" means any computer software or application that performs face surveillance.

"Government" means the State, or any of its political subdivisions, departments, agencies, and instrumentalities, corporate or otherwise.

"Government official" means any person or entity acting on behalf of the State, or any of its political subdivisions, including any officer, employee, agent, contractor, subcontractor, or vendor.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized.

"Written release" means informed written consent.

§ 2 Restriction on government use of face surveillance.

(a) Except as provided in subsection (b), it shall be unlawful
for the government or any government official to obtain, retain, access, or use:

(1) Any face surveillance system; or

(2) Any information obtained from a face surveillance system.

(b) A face surveillance system or information obtained from a face surveillance system shall only be obtained, retained, accessed, or used:

(1) By law enforcement agency personnel trained in the use of a face surveillance system;

(2) To compare surveillance photographs or videos to arrest booking photographs from the Hawaii criminal justice data center;

(3) In a photo lineup conducted pursuant to section 801K-2; and

(4) By driver's license and civil identification card issuing agencies to satisfy the requirements of the federal REAL ID Act of 2005.

Information obtained from a face surveillance system shall not constitute probable cause for an arrest.
§ 3 Restriction on private use of face surveillance without permission. (a) It shall be unlawful for any private entity to obtain, retain, access, or use any face surveillance system or any information obtained through a face surveillance system, unless the private entity first:

(1) Informs the subject or the subject's legally authorized representative in writing that the private entity wishes to obtain, retain, access, or use a face surveillance system or information obtained through a face surveillance system;

(2) Informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which the private entity wishes to obtain, retain, access, or use a face surveillance system or information obtained through a face surveillance system; and

(3) Receives a clear, discrete, written release, which is not a part of or otherwise combined with any other permission granting instrument or function, executed by the proposed subject of the face surveillance system or information obtained through a face surveillance system.
surveillance system or that subject's legally
authorized representative, granting permission to
obtain, retain, access, or use a face surveillance
system or information obtained through a face
surveillance system with respect to that subject.

(b) In the absence of a clear, discrete, written release
to do so, no private entity in possession of a face surveillance
system or information obtained through a face surveillance
system may sell, share, lease, trade, or otherwise profit from
information obtained through a face surveillance system.

(c) No private entity in possession of a face surveillance
system or information obtained through a face surveillance
system may disclose, redisclose, or otherwise disseminate
information obtained through a face surveillance system unless
the subject of the face surveillance system or information
obtained through the face surveillance system or the subject's
legally authorized representative consents to the disclosure,
redisclosure, or dissemination pursuant to the standards
contained in subsection (a).

(d) A private entity in possession of a face surveillance
system or information obtained through a face surveillance
system shall store, transmit, and protect from disclosure all
information obtained through a face surveillance system:

(1) Using the reasonable standard of care within the
private entity's industry; and

(2) In a manner that is the same as or more protective
than the manner in which the private entity stores,
transmits, and protects other confidential and
sensitive information.

(e) Nothing in this section shall be construed to prohibit
private entities from using cameras for internal security
related purposes; provided that any information collected from a
camera used for internal security related purposes shall not be
sold, shared, leased, traded, or otherwise profited from as
provided in this section.

§ 4 Enforcement. (a) Notwithstanding any other law to
the contrary, no data collected or derived from any use of a
face surveillance system 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 this State. Face surveillance data collected or
derived in violation of this chapter shall be considered
unlawfully obtained and shall be deleted upon discovery.

(b) 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 shall be brought against the respective
private entity or respective government, and, if necessary to
effectuate compliance with this chapter, any other governmental
agency with possession, custody, or control of data subject to
this chapter.

(c) Any person who has been subjected to face surveillance
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 private entity or government and shall
be entitled to recover actual damages, but not less than
liquidated damages of $100 for each violation or $1,000,
whichever is greater.
(d) A court shall award costs and reasonable attorneys' fees to a plaintiff who is the prevailing party in an action brought under subsection (b) or (c).

(e) Violations of this chapter by an employee of the government shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and the employee's collective bargaining agreement."

SECTION 3. This Act does not affect rights and duties that matured, penalties that were incurred, and proceedings that were begun before its effective date.

SECTION 4. This Act shall take effect on July 1, 2050.
Report Title:
Face Surveillance; Government Use; Private Use; Consent

Description:
Limits the government use of face surveillance except in certain circumstances. Limits the private use of face surveillance unless the subject of the face surveillance has given consent. Takes effect on 7/1/2050. (HD1)

The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.