DEPARTMENT OF THE PROSECUTING ATTORNEY

CITY AND COUNTY OF HONOLULU

ALII PLACE
1060 RICHARDS STREET • HONOLULU, HAWAII 96813
PHONE: (808) 768-7400 • FAX: (808) 768-7515

STEVEN S. ALM
PROSECUTING ATTORNEY

THOMAS J. BRADY
FIRST DEPUTY
PROSECUTING ATTORNEY

THE HONORABLE GREGG TAKAYAMA, CHAIR
HOUSE COMMITTEE ON HIGHER EDUCATION AND TECHNOLOGY
Thirty-First State Legislature
Regular Session of 2021
State of Hawai`i

February 5, 2021

RE: H.B. 1226; RELATING TO VIOLATION OF PRIVACY.

Chair Takayama, Vice Chair DeCoite, and members of the House Committee on Higher Education and Technology, the Department of the Prosecuting Attorney of the City and County of Honolulu ("Department") submits the following testimony in opposition to H.B. 1226.

The purpose of H.B. 1226 is to protect the privacy of Hawaii residents by placing limitations on facial surveillance to prevent possible unintended consequences from the rapidly evolving technology. Although this bill has good intentions, the Department believes that H.B. 1226 is premature and will have negative unintended consequences for law enforcement.

Prior to the 2020 Legislative Session, the Department had the good fortune to participate as a member of the Twenty-First Century Task Force ("Task Force"). The Task Force was established through House Concurrent Resolution No. 225 (2019) and was comprised of various members in the private and public sector who committed an extraordinary amount of time and effort in the construction of numerous legislative proposals. In fact, the Task Force took up the issue that is proposed in H.B. 1226 regarding the use of facial recognition software. After numerous discussions, the Task Force ultimately decided not to recommend legislation addressing what amounted to a non-problem. To date, facial recognition software is used as an investigative tool for law enforcement, but is never used to justify an arrest or the filing of a criminal charge. The Department is not aware of a single case where a person was charged or convicted of a crime as a result of facial recognition software. In fact, we are not aware of a single case in Hawaii where a person was mistakenly arrested as a result of the use of facial recognition software.

The Department is specifically concerned with the limitations placed on law enforcements use of arrest booking photos. On page 7, line 1-3, law enforcement is limited to only booking photos from the Hawaii Criminal Justice Data Center. **This provision severely limits the use of other valuable databases in Hawaii, but more importantly databases obtained and managed by the Federal Government and other states that are routinely used to assist in criminal**

investigations. The Department suggests expanding the language of this provision to ensure that law enforcement have the proper tools to properly investigate crimes that may be committed against Hawaii residents by individuals who may not live and reside in our state.

For all of the foregoing reasons, the Department of the Prosecuting Attorney of the City and County of Honolulu opposes the passage of H.B. 1226. Thank you for the opportunity to testify on this matter.

LATE

February 4, 2021

Hawaii House of Representatives
Committee on Higher Education and Technology

Subject: Written Testimony of the Security Industry Association in Opposition to HB 1226

Dear Chairman Takayama and Vice Chair DeCoite, and Members of the Committee:

On behalf of the Security Industry Association (SIA) and our members, I would like to share our concerns with the HB 1226 in its current form.

The Security Industry Association (SIA) is a nonprofit trade association representing businesses that provide a broad range of safety and security products for government, commercial and residential users in Hawaii and around the U.S. Our members include many of the leading manufacturers of facial recognition technology, as well as those who are integrating these technologies into a wide variety of building security and life-safety systems among other security solutions.

Support for Ensure Responsible, Ethical Use
We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Addressing concerns about public sector applications of facial recognition can and should be accomplished through policies ensuring appropriate transparency, procedures, oversight and other safeguards. We support policies ensuring that facial recognition is only used for appropriate purposes and in acceptable ways.[1]

Safety and Security Applications Undermined
As currently drafted, the bill under consideration would ban all current – and future – uses of facial recognition by government entities outside of several limited exceptions. A use case and application-specific approach to policymaking on facial recognition is critically important. For example, the bill preserves longstanding uses in criminal investigations, at airports and for reducing fraud in identification card issuance.

However, there are many other existing, non-controversial public sector uses Hawaii that fall outside these exceptions, which would be banned under the bill. Public concerns about facial recognition technology have centered around uses that raise privacy and civil liberties concerns, including law enforcement. However, other uses of the technology, such as in building systems, do not raise such concerns. The purpose is often simply to help validate one's identity, with obvious benefits to the users.

[1] See SIA's recommendations - https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

HOUSE OF REPRESENTATIVES
THIRTY-FIRST LEGISLATURE, 2021
STATE OF HAWAII

A BILL FOR AN ACT

RELATING TO VIOLATION OF PRIVACY.

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

SECTION 1. The legislature finds that the unregulated and unfettered use of facial recognition poses unique and significant implications with respect to the civil rights and liberties of residents of and visitors to Hawaii.

The legislature also finds that facial recognition technology is based upon algorithms that are known to vary in accuracy. For example, a 2019 study by the National Institute of Standards and Technology of the United States Department of Commerce found evidence of race-based biases in the majority of the facial recognition algorithms examined. The study found that Blacks, Asians, and Native Americans were particularly likely to be misidentified by lower-performing facial recognition algorithms~~technology~~. However, the same NIST study also found that the top-performing algorithms are over 99% accurate overall and across demographic groups and that they exhibited "undetectable" false positive error rate differentials across demographic groups.

The legislature further finds that facial recognition technology has already been used in concerning ways in other states and countries. This technology has reportedly been used to identify peaceful protestors during the 2020 Black Lives Matter protests in various cities. The use of this technology has also reportedly played a role in the false arrests of three Black men in the United States, with other possible erroneous arrests and convictions yet to be uncovered. In December 2020, *The New York Times* reported that one of the arrested men, Nijeer Parks, had his case dismissed for lack of evidence; he is now suing the police, prosecutor, and City of Woodbridge, New Jersey, for false arrest, false imprisonment, and violation of his civil rights. Additionally, at least one foreign government is reported to have complete facial recognition profiles on all its citizens, which the government uses without restraint to suppress free speech and invade the privacy of people within its borders. Although that foreign government is an authoritarian regime without the Constitutional rights that underpin American democracy, the legislature wants to strengthen Hawaii's privacy protections and believes that Hawaii's citizens should not be subject to such violations of privacy.

The legislature also finds that the broad application of government facial recognition in public spaces is the functional equivalent of requiring every person to carry and display a personal photo identification card at all times and to carry a

government global positioning system tracking device, which would constitute an unacceptable violation of privacy.

The legislature further believes, however, that there are limited circumstances in which the use of facial recognition does not infringe on an individual's privacy rights. Some county police departments have used facial recognition 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 that already exist in the Hawaii criminal justice data center's database. The facial recognition program is intended to identify possible suspects by generating investigative leads for detectives, but any identification cannot constitute probable cause for arrest. The legislature believes that county police departments should be allowed to continue to use facial recognition for this limited passive purpose. However, the legislature finds that further uses of facial recognition technology should be prohibited unless vetted and approved by the legislature.

The legislature further finds that the airports division of the department of transportation plans to use facial recognition technology to identify persons passing through airports who have fevers and may be infected with coronavirus disease 2019 (COVID-19) or other infectious diseases that pose a public health risk to the State. The legislature believes that monitoring passengers is a necessary step to ensure that

Hawaii's economy can fully function while keeping the public safe. The legislature believes that the airports division of the department of transportation should be allowed to continue to use facial recognition technology for this emergency purpose solely within airports. However, any monitoring must be properly balanced with the constitutional right to privacy, the immediate destruction of obtained data that is no longer necessary to retain, and limitations on sharing that data.

The purpose of this Act is to ensure that the legislature has the opportunity to properly vet future uses of rapidly evolving facial recognition technology and to prevent unintended consequences from interfering with the privacy and freedom of persons in the State, as has occurred in other jurisdictions, by placing limits on the government's use of facial recognition systems, with certain specified exceptions.

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

"CHAPTER

FACIAL RECOGNITION PROHIBITION

§ -1 Purpose and scope. The purpose of this chapter is to help ensure that government's use of facial recognition systems promotes privacy and other civil rights and civil liberties, social justice, safety, security, efficiency, and innovation.

§ **-2 Applicability.** This chapter shall not apply to a government official's personal use of a privately owned facial recognition system when the government official is acting in an unofficial capacity.

§ **-3 Definitions.** As used in this chapter:

"Facial recognition" means includes all of the following:

(1) Facial identification technologies, which identify an individual by generating a mathematical representation of the individual's face, known as a facial template, searching a database populated with many facial templates linked to personally identifiable information (PII) for a matching template, and returning an identity if the probe facial template matches any facial template in the database

(2) Facial verification technologies, which confirm an individual's identity by comparing a probe facial template to a single, specific facial template linked to PII in a database;

(3) Facial characterization technologies, which generate and analyze a facial template that is not linked to PII to determine an individual's demographic characteristics or emotional state

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

"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.

§ -4 Restriction on government use of facial recognition. (a) Except as provided in subsection (b), until the use is approved according to the process in subsection (c), it shall be unlawful for the government or any government official to obtain, retain, share, access, or use:

(1) Any facial recognition system; or

(2) Any information obtained from a facial recognition system.

(b) Without gaining approval according to the process in subsection (c), a facial recognition system or information obtained from a facial recognition system shall only be obtained, retained, shared, accessed, or used in accordance with the requirements in subsection (d) and:

(1) By law enforcement agency personnel trained in the use of a facial recognition system:

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

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

(2) By driver's license and civil identification card issuing agencies to help combat fraud or satisfy the requirements of the federal REAL ID Act of 2005, Public Law 109-13; or

(3) By the government or a government official at state airports:

(A) To facilitate commercial airline or airport programs or Federal Government programs; or

(B) Upon a determination by the director of health that there is a potential for a serious outbreak of a communicable or dangerous disease or there is the likelihood of extensive injury or death;

(i) At state airports;

(ii) In conjunction with thermal scanning health technology; and

(iii) To identify an individual when there is reason to believe, based on thermal scanning technology, that the individual could be infected with a communicable or dangerous disease;

provided that information obtained from a facial recognition system shall be destroyed within fourteen days of the date on which the individual's health status ahs been ascertained..

4 (c)(1) The Attorney General shall approve new facial recognition uses when, and only when, they satisfy the following requirements:

(A) At least ninety days before the planned facial recognition deployment is set to become operational, a government official intending to use a facial recognition system shall post a public notice on its website detailing:

(i) the planned use of facial recognition;

(ii) the purpose for the use;

(iii) the specific facial recognition system and vendor that the government official plans to use;

(iv) test results from a current National Institute of Standards and Technology (NIST) report, another federal government study, or other equally

robust third-party information about the facial recognition system's accuracy overall and across demographic groups;

(v) a certification indicating that the government official has satisfied any applicable Information Privacy and Security Council (IPSC) data privacy requirements, data breach requirements, or other best practice requirements;

(vi) the plans for training government officials to operate the facial recognition system; and

(vii) the government official's statement of intent to comply with the requirements in subsection (d).

(B) The government official shall provide an opportunity for public comment in response to the posted notice.

(C) Within sixty days of the close of the public comment period, the government official shall post a statement or take other actions to respond to the public comments.

(2) If a public health or other state emergency exists, a government official may obtain a temporary approval process waiver that would allow immediate use of facial recognition for the limited purpose of helping to combat the emergency. In such an emergency situation, the government official would still be responsible for completing the approval process within a reasonable time period after obtaining the temporary approval process waiver.

(d)(1) Every two years, a government official using a facial recognition system must submit an accountability report detailing the use of that facial recognition system to the Attorney General by the close of the fiscal year.

(A) This biannual accountability report shall include:

(i) The name of the facial recognition vendor;

(ii) Test results from a current National Institute of Standards and Technology (NIST) report, another federal government study, or other equally robust third-party information about the facial recognition system's accuracy overall and across demographic groups;

(iii) Plans to upgrade the facial recognition system on a regular basis to promote accuracy overall and across demographic groups;

(iv) The government official's policy governing the use of the facial recognition system and the management of data from the facial recognition system and any planned updates to that policy;

(v) Information about how the government official has been using the facial recognition system to collect and process data and any changes to the scope of the original purpose for which the government official planned to use the facial recognition system;

(vi) Information about the facial recognition system's performance and any measures that the government official has taken or plans to take to address any identified performance issues;

(vii) Information about training to ensure compliance with policies governing the use of the facial recognition system and the management of data from the facial recognition system;

(viii) Any known or reasonably suspected violations of the policy governing the use of the facial recognition system and the management of data from the facial recognition system and any actions taken in response to the known or reasonably suspected violations.

(ix) Information about the government official's efforts to ensure that the use of the facial recognition system does not negatively impact privacy or other civil rights and civil liberties.

(B) The government official shall post a public summary of the accountability report on its website within ninety days of submitting of the report to the Attorney General and shall provide an opportunity for public comment. Within sixty days of the close of the public comment period, the government official shall post a statement or take other actions to respond to the public comments.

(2) Information obtained from a facial recognition system shall not, on its own, constitute probable cause for an arrest."

SECTION 3. This Act shall take effect upon its approval.

INTRODUCED BY: _____

Report Title:
Privacy; Facial Recognition Systems; Government Officials; Limitations on Use

Description:
Limits the government's use of facial recognition systems, except in certain circumstances. Does not apply to personal use of a privately owned facial recognition system when acting in an unofficial capacity.