STATE OF HAWAI‘I
OFFICE OF THE PUBLIC DEFENDER

Testimony of the Office of the Public Defender,
State of Hawai‘i to the Senate Committee on Public Safety,
Intergovernmental, and Military Affairs

February 8, 2020

S.B. No. 3148: RELATING TO FACE SURVEILLANCE

Chair Nishihara, Vice Chair Wakai, and Members of the Committee:

The Office of the Public Defender strongly supports S.B. 3148.

The rapid development and proliferation of facial recognition technology and recent evaluations of this technology have been a seriously cause for concern. This accuracy of this technology has yet to be fully vetted and is highly dependent on the accuracy of the data entered into the software or algorithms used by each system. We are deeply concerned about the very real biases that these systems have yet to protect against -- racial bias, gender bias and age bias. The technology has yet to reach the sophistication to check for or eliminate systematic problems with these types of biases and there are far too many instances of false positives to render the technology as reliable unless images entered into the system are clear, unblurred, and still. Many images, whether still or moving, may be blurred, grainy, and under circumstances where poor lighting, awkward angles, or partial images are captured.

We support S.B No. 3148 and agree that "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." (*see* page 3, lines 3-6).

We also submit for your review and consideration two recent articles on facial recognition technology that support our concerns:

- National Institute of Standards and Technology, NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software (December 19, 2019) (https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software (last visited, February 8, 2020)

- Valentio-DeVries, Jennifer, The New York Times, How the Police Use of Facial Recognition, and Where It Falls Short (January 12, 2020) (https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html (last visited, February 8, 2020)

Thank you for the opportunity to comment on this measure.

DAVID Y. IGE
GOVERNOR

CURT T. OTAGURO
COMPTROLLER

AUDREY HIDANO
DEPUTY COMPTROLLER

STATE OF HAWAII
DEPARTMENT OF ACCOUNTING AND GENERAL SERVICES
P.O. BOX 119, HONOLULU, HAWAII 96810-0119

WRITTEN TESTIMONY
OF
CURT T. OTAGURO, STATE COMPTROLLER
DEPARTMENT OF ACCOUNTING AND GENERAL SERVICES
TO THE
SENATE COMMITTEE ON
PUBLIC SAFETY, INTERGOVERNMENTAL AND MILITARY AFFAIRS

TUESDAY, FEBRUARY 11, 2020, 2:00 P.M.
CONFERENCE ROOM 229, STATE CAPITOL

S.B. 3148

RELATING TO FACE SURVEILLANCE

Chair Nishihara, Vice Chair Wakai and Members of the Committees, thank you for the opportunity to testify on S.B. 3148.

The Department of Accounting and General Services (DAGS) opposes S.B. 3148 which prohibits government use of face surveillance other than existing police department use; and prohibits private use of face surveillance unless the subject of the face surveillance has given clear, discrete, written consent.

The DAGS manages 74 state facilities which includes facilities in the State Capitol District. A major concern that we face in managing facilities is keeping our tenants and employees safe. A good example is the Hawaii State Capitol which is one of the most open and welcoming State Capitols in the country but is also one of the least secure. The DAGS is committed to keeping its tenants and employees safe using the most advanced tools and resources available. In addition, Facial Recognition (FR) technology can be used to improve safety and security for State employees and State lawmakers at State facilities. The DAGS offers the following comments:

1. FR technology has not fully matured and there may be applications that may serve our tenants and employees without violating individual privacy. There is no provision that allows for flexibility to use facial recognition solution where privacy violation objections may be addressed. In lieu of outlawing the technology, we recommend outlawing the storing of information, obtained by the technology, and other actions that the legislature deems is in violation of a person's privacy rights. This would allow the use of the technology to identify the presence of people of risk and allow security to take the proper precautions without storing any personal identifying information.
2. Facial recognition cannot operate independent of the existing surveillance platforms that exist today. The continuous tracking and monitoring correlated with other system data would require a separate analytics/AI engine and/or human (LEO) operators to aggregate data. This threat actually exists in the form of the smartphone, as companies with access to the device data (e.g. Facebook, Verizon, google, ATT, app developers) have a personally identifiable device that is always on and can be tracked to the foot (including usage of the device for anything online). Smartphone based profiles include age, gender, and location. Facial recognition-based solutions can only provide yes/no to another tool.
3. Restricting government use of facial recognition to existing police department use would limit the resources and tools available to other state agencies. FR technology has applications to improve safety and security for State employees and State lawmakers. In addition, Public Safety Department facilities and Department of Health State hospitals would benefit from FR through improved safety and security.
4. SECTION 2. (b) Amend lines 3-12 on Page 6:

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

(3) In a photo lineup conducted pursuant to section~~.~~;

(4) For other future public safety applications;

(6) For protection of public gatherings where mass violence threats exist; and

(7) For protection of government facilities and employees."

Thank you for the opportunity to submit testimony on this matter

POLICE DEPARTMENT

CITY AND COUNTY OF HONOLULU

801 SOUTH BERETANIA STREET · HONOLULU, HAWAII 96813
TELEPHONE: (808) 529-3111 · INTERNET: www.honolulupd.org

KIRK CALDWELL
MAYOR

SUSAN BALLARD
CHIEF

JOHN D. McCARTHY
CLYDE K. HO
DEPUTY CHIEFS

OUR REFERENCE WO-KK

February 11, 2020

The Honorable Clarence K. Nishihara, Chair
and Members
Committee on Public Safety,
Intergovernmental, and Military Affairs
State Senate
Hawaii State Capitol
415 South Beretania Street, Room 229
Honolulu, Hawaii 96813

Dear Chair Nishihara and Members:

SUBJECT: Senate Bill No. 3148, Relating to Face Surveillance

I am Walter Ozeki, Major of the Criminal Investigation Division of the Honolulu Police Department (HPD), City and County of Honolulu.

The HPD opposes Senate Bill No. 3148, Relating to Face Surveillance.

While the HPD is familiar with the various published studies related to the use of face surveillance technology and with the objections raised by the American Civil Liberties Union and similar organizations, it is of note that because the technology associated with the use of face surveillance is fairly new and quickly evolving, there are no federal regulations on the use of this technology.

With this in mind and citing this bill itself, "One known advantage of face surveillance in Hawaii is that some county police departments have used face surveillance technology in a limited capacity..." and "While the face surveillance program is relatively new and has been used relatively few times, the results of the program has been promising," it is the HPD's position that it is premature to provide blanket regulations on the use of face surveillance technology by law enforcement. At this time, we do not have any indication as to how quickly this technology may advance and how valuable these advances may prove to be in the near future.

Law enforcement is already approaching the use of face surveillance in a cautious and responsible manner, and it is the judiciary that would ultimately make the final determination of the admissibility of face surveillance evidence based on the constitution and established case law.

The HPD urges you to oppose Senate Bill No. 3148, Relating to Face Surveillance.

Thank you for the opportunity to testify.

Sincerely,

Walter Ozeki, Major
Criminal Investigation Division

APPROVED:

Susan Ballard

Susan Ballard
Chief of Police

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

February 10, 2020

Senator Clarence K. Nishihara, Chair
Committee on Public Safety, Intergovernmental, and Military Affairs

Re: S.B. 3148 Relating to Face Surveillance
Hearing: Tuesday, February 11, 2020 at 2:00 p.m.
Conference Room: 229

Dear Chair Nishihara and Members of the Committee on Public Safety, Intergovernmental, and Military Affairs:

At Microsoft, we believe in the power of advancing technology to bring important and exciting societal benefits. But we also recognize that as with all tools, technology has the potential to be misused. As technology companies create new and innovative technologies that are rapidly changing the world, they also have an obligation to help address the challenges and concerns that such changes bring. Facial recognition is one such technology that both offers tremendous benefits but also raises serious issues that call for thoughtful government regulation.

Facial recognition—which generally refers to the ability of a computer to recognize people's faces from a photo or video—is a powerful tool that offers a range of important benefits. As the technology develops, it could be used to find missing persons, thwart terrorism, diagnose rare genetic conditions, and assist the blind. At the same time, as with any tool, it also holds the potential for misuse by both private companies and public authorities.

Potential misuses need to be addressed

The potential for misuse is real. We believe there at least three problems that governments need to address: (1) use of facial recognition technologies that lead to biased and potentially discriminatory outcomes; (2) widespread intrusions on people's privacy; and (3) mass surveillance that threatens to chill democratic freedoms. For example, without a thoughtful approach to facial recognition technology, law enforcement may rely on flawed or biased technological approaches to decide who to track, investigate, or even arrest for a crime. Governments may monitor the exercise of political and other public activities in ways that conflict with our democratic principles, chilling our core freedoms of assembly and expression. Similarly, companies may use facial recognition to make decisions that affect credit eligibility, employment opportunities, or purchasing behavior. These are important considerations of privacy, free speech, freedom of association, and even life and liberty.

Biases and inaccuracies need to be mitigated

These concerns are heightened for many marginalized communities. For example, some facial recognition technologies have been found to work more accurately for white men than for women or people of color. While researchers across the tech sector are working to address these challenges and significant progress is being made, deficiencies remain. And even if biases are mitigated and facial recognition systems operate in a manner deemed fairer for all people, we will still face challenges, as with many AI technologies, of potential failures. These challenges call for meaningful human review where facial recognition systems may be used to make important decisions, including those that result in the denial of consequential services such as housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.

Regulation should permit responsible government and commercial use of facial recognition

Some believe that these challenges necessitate an outright ban use. From our perspective, a general ban or moratorium would go too far—thwarting the benefits of this technology. Rather, we believe thoughtful legislation can provide protections and guardrails to help ensure due process and fair use of facial recognition technologies in both the government and commercial contexts. For example, we support legislation that requires testing prior to use and ensuring a human reviews important decisions impacting individuals. Facial recognition that is not fit for the purpose for which it is being deployed should not be used.

To strike an appropriate balance, Microsoft believes that legislation should be based upon the standards listed below regarding how and when companies can use facial recognition technology.

- **Fairness:** Suppliers of facial recognition technology must build their technology so that independent third parties can test its accuracy and examine it for unfair biases and inaccuracies across subpopulations. Companies must be required to take action when undisclosed problems with the technology are discovered and must be transparent about the capabilities and limitations of their technology.
- **Notice and Consent:** In any public place where facial recognition technology is used, companies must post clear notice. And as a default, companies must obtain meaningful consent from individuals before adding their image to a facial recognition database.
- **Human Review**: Accuracy must be a shared responsibility between the companies that develop facial recognition technology and the organizations that use it. Facial recognition alone should not be used to make legal or critical decisions like mortgage approval or job consideration; humans must be involved in the decision-making process.

It also critical to regulate the use of facial recognition by the government. Many of the safeguards that apply to corporate use should also apply specifically to government scenarios. For example, to protect due process, ongoing surveillance with facial recognition should only be used in public places to address a serious crime where a search warrant has been issued, or in the circumstance of a true emergency like a terrorist threat or a kidnapped child. Further, legislation should require law enforcement to disclose to an accused anytime facial recognition is used in a legal case against them.

These principles provide strong baseline standards that will give people meaningful protections and will provide a solid foundation for legislators to build and improve upon them. If action is not taken, we risk waking up five years from now (or even sooner) to find that facial recognition services have spread in ways that exacerbate existing societal problems.

Moving forward

The Hawaii legislature has an opportunity to establish appropriate standards for the use of facial recognition technology and Microsoft supports the discussion that the legislature has initiated on this important subject. To ensure society can realize the benefits of facial recognition while also addressing the challenges it poses around potential misuse, we encourage the Hawaii legislature to include provisions around fairness, notice and consent and human review, as outlined above. We also believe that the discussion of these challenging and important issues requires input from stakeholders across society.

We look forward to contributing to this conversation and would be happy to discuss these issues with you in more detail as the conversation develops. Thank you for your consideration.

Sincerely,

Jonathan Noble
US Government Affairs
Microsoft

DAVID Y. IGE
GOVERNOR

LATE

TESTIMONY BY:

JADE T. BUTAY
DIRECTOR

Deputy Directors
LYNN A.S. ARAKI-REGAN
DEREK J. CHOW
ROSS M. HIGASHI
EDWIN H. SNIFFEN

STATE OF HAWAII
DEPARTMENT OF TRANSPORTATION
869 PUNCHBOWL STREET
HONOLULU, HAWAII 96813-5097

February 11, 2020
2:00 P.M.
State Capitol, Room 229

S.B. 3148
RELATING TO FACE SURVEILLANCE

Senate Committee on Public Safety, Intergovernmental, and Military Affairs

The Department of Transportation **supports with amendments** S.B. 3148, which limits the government use of face surveillance except in certain circumstances and limits the private use of face surveillance unless the subject of the face surveillance has given consent.

The bill needs to be amended to allow driver's license and state identification card (SID) issuing agencies to perform "face surveillance" as the terminology is defined in the bill. The driver's license and SID issuing agencies must perform a face recognition check to ensure that the individual holds only one of these credentials in the state. This is a requirement of the REAL ID Act and Hawaii meets the Department of Homeland Security Final Rules requirement by using facial recognition technology. Failure to allow this will jeopardize Hawaii's REAL ID compliance status and will affect how the driver's license and SID are accepted by airport and federal facility security screening.

SECTION 2, new section -2, which begins on page 5, line 17 should be amended as follows:

§ -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) Face surveillance technology 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 face surveillance technology;

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

(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.

Thank you for the opportunity to provide testimony.

DEPARTMENT OF THE PROSECUTING ATTORNEY

CITY AND COUNTY OF HONOLULU

ALII PLACE
1060 RICHARDS STREET • HONOLULU, HAWAII 96813
PHONE: (808) 547-7400 • FAX: (808) 547-7515

DWIGHT K. NADAMOTO
ACTING PROSECUTING ATTORNEY

LYNN B.K. COSTALES
ACTING FIRST DEPUTY
PROSECUTING ATTORNEY

LATE

THE HONORABLE CLARENCE K. NISHIHARA, CHAIR
SENATE COMMITTEE ON PUBLIC SAFETY, INTERGOVERNMENTAL, AND MILITARY AFFAIRS
Thirtieth State Legislature
Regular Session of 2020
State of Hawai`i

February 11, 2020

RE: S.B. 3148; RELATING TO FACE SURVEILLANCE.

Chair Nishihara, Vice Chair Wakai, and members of the Senate Committee on Public Safety, Intergovernmental, and Military Affairs, the Department of the Prosecuting Attorney of the City and County of Honolulu (the Department) submits the following testimony in opposition of S.B. 3148.

Last year, pursuant to House Concurrent Resolution 225, the Hawaii State Legislature created the 21st Century Privacy Law Task Force. This task force addressed a number of privacy issues facing Hawaii. However, despite various discussions regarding facial recognition technology, the task force did not submit any policy or legislative recommendations in relation to facial recognition. Therefore, S.B. 3148 is not a byproduct of the task force and as drafted, S.B. 3148 fails to address a number of concerns by the Department.

The Department is greatly concerned that as drafted, S.B. 3148 fails to define the most important term – “surveillance”. This is problematic as it appears numerous times throughout the bill (ie. face surveillance, face surveillance system, and surveillance photograph) and could create a constitutional issue of being too vague and overbroad. Specifically, this bill creates the unintended consequence of subjecting every individual using a cellphone, camera or video camera to potential lawsuits. With today’s technological advances, most cellular phones, video cameras and personally owned cameras have the ability to capture information about a person’s physical characteristics, such as their face. Currently S.B. 3148 defines “face surveillance” to include “any process that captures information about an individual based on the physical characteristics of the individual’s face” and further incorporates the broad definition to “private entities” which essentially applies to every individual (pg. 7, line 13-15 – “any individual, partnership, corporation, limited liability company, association, or other group however organized"). Under the plain language of S.B. 3148, every person who uses a device (like a cell phone) operated by software (like cell phones and digital cameras and video recorders) who may "capture information about an individual based on the physical characteristics of the individual's face" would need a "written release" before "capturing information about another person's physical characteristics, like their face. Further, an individual who shares the image or someone's face without first obtaining written consent would also be in violation of S.B. 3148 and subject to a potential lawsuit. Lastly, this bill could lead to needless litigation and loss of otherwise valuable investigative evidence due to the remedies outlined on page 9, line 3 relating to suppression as an enforcement mechanism.

The Department would note to this committee that facial recognition technology is subject to an existing framework of laws, regulations, and administrative rules and best practices that already address the concerns of the proponents of this bill. Most significant is that Hawaii residents cannot be misidentified by facial recognition technology errors due to the fact that the technology does not identify perpetrators – humans do when they view photo lineups and live lineups. Moreover, the suggestion that facial recognition technology has an inherent racial bias is not factual. In fact, recent research by the NIST indicates that newer software algorithms have accuracy rates for African Americans equal to or even higher than for other groups. According to the NIST, between 2014 and 2018, facial recognition software got 20 times better overall at searching a database to find a matching photograph. After testing 127 software algorithms from 39 different developers, the combined failure rate was just 0.2 percent, meaning that systems were 99.8 percent accurate compared to 96 percent accurate four years before.

For these reasons, the Department of the Prosecuting Attorney opposes the passage of S.B. 3148. Thank you for this opportunity to testify.

ACLU
Hawai‘i

LATE

Committee:	Committee on Public Safety, Intergovernmental, and Military Affairs
Hearing Date/Time:	Tuesday, February 11, 2020, 2:00 p.m.
Place:	Conference Room 229
Re:	*Testimony of the ACLU of Hawai‘i* ***with comments on*** *S.B. 3148, Relating to Face Surveillance*

Dear Chair Nishihara, Vice Chair Wakai, and Committee Members:

The American Civil Liberties of Hawai‘i ("ACLU of Hawai‘i") offers comments on S.B. 3148, which would limit government use of facial recognition technology ("FRT"), except as provided in subsection 2(b), and would ban private entities' use of this technology unless the subject has given clear, written consent. The ACLU of Hawai‘i supports every provision of this bill except for subsection 2(b), which we request be stricken entirely. Alternatively, the ACLU of Hawai‘i proposes an amendment, below, to ensure that FRT used by law enforcement does not carry racial or gender bias. S.B. 3148, if amended, would safeguard Hawaii's residents against dangerous, invasive, and biased systems that threaten civil rights and safety.

Subsection 2(b) should be stricken entirely or amended to prevent racial or gender bias in policing.

It is the understanding of the ACLU of Hawai‘i that Honolulu Police Department (HPD) has already adopted this technology without any meaningful community input. HPD requires reasonable suspicion to run a face recognition search, with the exception for "requests that come directly from the Chief."[1] Right now, it is unclear whether searches can be run on witnesses or bystanders. Searches compare persons in photos or videos to existing booking photos.[2] The State has determined that current statutes, rules, and regulations prohibit driver's license and ID card photos from being included in the FRT.[3]

The costs of this technology to both civil rights and civil liberties substantially and categorically outweigh any benefits. **For this reason, the ACLU of Hawai‘i respectfully requests that the bill's provision exempting HPD's existing use of FRT—subsection 2(b)—be stricken entirely.** If the Committee is inclined to retain subsection 2(b), we ask that, a minimum, the following language be

[1] Garvie, C., Bedoya, A., Frankle, J. (2016, October 8). The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy and Technology. Retrieved from https://www.perpetuallineup.org/jurisdiction/hawaii

[2] Honolulu Police Department Policy Auxiliary and Technical Services, Policy Number 8.21, September 14, 2015 Retrieved from https://www.honolulupd.org/information/pdfs/FacialRecognitionProgram-02-04-2016-12-19-14.pdf

[3] Garvie, Bedoya, and Frankle, *supra*. *See* Attachment 016846, statement by Hawai‘i Criminal Justice Data Center Representative via email correspondence with Clare Garvie regarding the Driver's Privacy Protection Act and Real ID Act protections against FRT

inserted into the bill to ensure that technology used by law enforcement does not carry racial or gender bias:

"The permissible uses provided for in subsection 2(b) shall only be allowed where the face surveillance technology or the face surveillance system from which the information is obtained has been demonstrated, through independent testing, to produce no greater rates of false positive identifications for any class of persons protected by the constitutions and laws of the United States of America and State of Hawaii."

The science behind FRT is far from perfect.

FRT is used to verify the identity of a person using facial characteristics. Algorithms determine distinctive details of each face—for example, the distance between the eyes or shape of the chin. This information is converted into a mathematical representation, given a template, and stored in a database.[4] Photos collected of an individual via social media, police body cameras, surveillance cameras, traffic cameras, or in the field, are run against face templates in the database using algorithms that rely on facial markers to find the closest match. However, instead of yielding a single matching result, the system offers up several potential matches ranked in the order of likelihood of closest identification, which is problematic. FRT is also heavily reliant on "perfect" conditions and produce negative results in poor lighting conditions, low resolutions, faulty angles, and etc. FRT's optimal performance relies on booking photo quality photographs with good lighting and from a frontal perspective.[5] When photographs are compared to those that have different lighting, shadows, backgrounds, poses, or expressions, misidentification rates increase.[6] Identifying someone under low resolution or a in a video footage also poses the same issues.

Fourth Amendment and First Amendment rights are at stake.

The City and County of Honolulu recently approved increased surveillance in its tourist district and are working towards establishing more surveillance in its public parks. Even if people are not suspected of a crime, meeting certain physical attributes that society considers "threatening" (like engaging in political protest in public spaces) is sufficient to garner the attention of law enforcement. Hawaii's own history during World War II is a stark reminder that gathering data based on people's race, ethnicity, religious beliefs, and political leanings, often leads to misuse, injustice, and the deterioration of civil rights and civil liberties protections.[7] The powerful and automated nature of FRT result in needless expansion of surveillance in communities. People should not have to be wary of having their private lives recorded when walking down the street. As a result, FRT can have a real chilling effect on people's willingness to engage in civic duties, participate in religious events, or

[4] Lynch, J. (2018, February 12). Face Off: Law Enforcement Use of Face Recognition-Technology. Retrieved from https://www.eff.org/wp/law-enforcement-use-face-recognition.

[5] *Id*.

[6] Phillips, J., Beveridge, R., Draper, B., et al. An Introduction to the Good, the Bad, & the Ugly Face Recognition Challenge Problem. Retrieved from https://www.nist.gov/itl/iad/ig/upload/05771424.pdf

[7] Cohen, A. (2011, May 5) Treatment of Japanese-Americans in WWII Hawaii Revealed in Article Retrieved from https://www.law.berkeley.edu/article/treatment-of-japanese-americans-in-wwii-hawaii-revealed-in-article/

engage in free speech.

FRT threatens the civil rights of communities of color and women.

A study by the ACLU of Northern California reveals that FRT marketed to law enforcement mistakenly matched the faces of one out of five lawmakers with images from an arrest photo database. More than half of the falsely identified are lawmakers of color, illustrating the most dangerous risk of FRT. A similar ACLU test conducted in 2018 also misidentified 28 sitting members of Congress. There are also studies that reveal the inaccuracies when used on women and people of color. An identification — whether accurate or not — could cost people their freedom or even their lives.

Other jurisdictions have adopted similar laws to protect their residents.

In May 2019, the city of San Francisco became the first city to prohibit government acquisition and use of FRT. Since then, the cities of Oakland, Berkley, Somerville, Cambridge have introduced and adopted similar legislation. More cities and states are beginning to understand the dangers and concerns of FRT and more will soon follow. Recently, the State of California successfully enacted a landmark law that blocks law enforcement from using FRT on body cameras. In 2008, Illinois passed the Biometric Information Privact Act,[8] which restricts private use of FRT and is substantially similar to subsection three of S.B. 3148. In light of the highly invasive collection of millions of people's biometric information by private companies,[9] prohibitions on private use are necessary.

It is integral that privacy protections keep up with technological advancements to ensure that the State of Hawaii continues to uphold our explicit constitutional right to privacy. We must reclaim control of our information; for when privacy is at stake, free speech, security, and equality will soon follow. For this reason, the ACLU of Hawaiʻi requests that the Committee support this measure, with our proposed amendments.

Thank you for the opportunity to testify.

Sincerely,

Mandy Fernandes
Policy Director
ACLU of Hawaiʻi

The mission of the ACLU of Hawaiʻi is to protect the fundamental freedoms enshrined in the U.S. and State Constitutions. The ACLU of Hawaiʻi fulfills this through legislative, litigation, and public education programs statewide. The ACLU of Hawaiʻi is a non-partisan and private non-profit organization that provides its services at no cost to the public and does not accept government funds. The ACLU of Hawaiʻi has been serving Hawaiʻi for 50 years.

[8] 740 ILCS 14, Biometric Information Privacy Act.

[9] *See*, *e.g.*, Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, New York Times (Jan. 18, 2020), *available at* https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

SB-3148
Submitted on: 2/10/2020 6:13:05 PM
Testimony for PSM on 2/11/2020 2:00:00 PM

LATE

Submitted By	Organization	Testifier Position	Present at Hearing
Charles Lotsof	Individual	Oppose	Yes

Comments:

The shortcoming with this proposed law is that it needlessly and totally bans the use of identity recognition devices that actually can be and commonly are used for extraordinarily good purposes.

Suppose for example that a membership store like Costco gets alerted that the free samples of an edible product it has been giving out that day to customers, have a contamination that will cause alarming symptoms starting 2 hours after ingestion but lasting only for 15 minutes. The store has the equipment with facial recognition technology to compare with store video showing customers lined up for the samples with file head, and shoulders pictures of all their customer-members. A program can be run to identify every potential victim in time to alert him not to panic. Under the terms of the proposed law, using that technology would be illegal.

There is nothing wrong with capturing information about a individual’s appearance based on the physical characteristics of the individual's face; it can be used for highly beneficial purposes. It is the use of this same technology for nefarious, ulterior purposes that is so ill-conceived and that this overly broad statute should be designed to prevent. Totally outlawing this technology regardless of the purpose would be reprehensible.

The popular website https://www.google.com/imghp?hl=en can be used in identifying or verifying the identity of an individual by uploading a picture of an individual. As written, this bill would ban accessing this website to obtain information identifying a person without his consent.