



**WRITTEN TESTIMONY OF  
THE DEPARTMENT OF THE ATTORNEY GENERAL  
THIRTIETH LEGISLATURE, 2020**

---

**ON THE FOLLOWING MEASURE:**

S.B. NO. 3148, S.D. 1, RELATING TO FACE SURVEILLANCE.

**BEFORE THE:**

SENATE COMMITTEE ON JUDICIARY

**DATE:** Thursday, February 27, 2020      **TIME:** 10:15 a.m.

**LOCATION:** State Capitol, Room 016

**TESTIFIER(S):**      **WRITTEN TESTIMONY ONLY.**  
(For more information, contact Lori N. Tanigawa,  
Deputy Attorney General, at 586-0618)

---

Chair Rhoads and Members of the Committee:

The Department of the Attorney General provides the following comments.

The purposes of this bill are to limit the government use of face surveillance except under certain circumstances and to limit the private use of face surveillance unless the subject of the face surveillance has given consent.

The Hawaii Criminal Justice Data Center (HCJDC) is responsible for the collection, storage, dissemination, and analysis of all pertinent criminal justice data and related functions. In particular, HCJDC is responsible for the Automated Biometric Identification System (ABIS), which stores fingerprints and facial images that are used by State and county law enforcement agencies. HCJDC contracts with a private vendor to furnish, operate, and maintain the software that stores the facial images, the application used to run a facial comparison, and the ABIS server that houses the data. HCJDC therefore requires access to perform its statutory duties, and HCJDC's vendor requires access for user-support and maintenance purposes. In addition, it should be noted that agencies may require access to comply with federal law and that federal agencies may require access to ensure compliance with federal law. We therefore recommend that new section -2(b) on page 6, lines 3 to 16, of the bill be amended as follows:

(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;
- (3) In a photo lineup conducted pursuant to section 801K-2;
- (4) For other future public safety applications;
- (5) For protection of public gatherings where mass violence threats exist; ~~and~~
- (6) For protection of government facilities and employees~~[-]~~;
- (7) By the Hawaii criminal justice data center for purposes of carrying out its duties and obligations, as set forth in chapter 846;
- (8) By contractors of the Hawaii criminal justice data center for operation and maintenance purposes; and
- (9) As required by federal law or as necessary to assist federal agencies in ensuring compliance with federal law.

The bill requires a private entity in possession of a face surveillance system or information obtained through a face surveillance system to store, transmit, and protect from disclosure all such information in accordance with two standards. We believe there is a potential for the standards to conflict and therefore suggest that new section -3(d)(1) and (2) on page 9, lines 1 to 6, of the bill be amended as follows:

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

Because claims against the government are governed by different standards and legal principles than claims against private parties, we recommend that the bill be amended to differentiate between enforcement actions against the government and enforcement actions against private parties. In addition, we recommend that subsections (d) and (e) be amended to allow for greater flexibility in their implementation given that there may be other circumstances which may affect the

award of costs and attorneys' fees and personnel decisions. We therefore suggest that page 9, lines 17 to 21, and page 10, lines 1 to 20, of the bill be amended as follows:

(b) Any person who has been subjected to face surveillance by the government in violation of this chapter [~~constitutes an injury and any person~~] or about whom information has been obtained, retained, accessed, or used by the government, may institute proceedings for injunctive relief[, ~~declaratory relief, or writ of mandate~~] in [any] circuit 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 by a private entity in violation of this chapter or about whom information has been obtained, retained, accessed, or used by a private entity in violation of this chapter, may institute proceedings in any court of competent jurisdiction against the private entity [~~or government and~~] for damages or equitable relief. A person who prevails in an action brought under this subsection shall be entitled to recover actual damages[, ~~but no less than liquidated damages of~~] or \$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) shall be entitled to reasonable costs and attorneys' fees.

(e) Violations of this chapter by an employee of the government [~~shall~~] may result in consequences, [~~that may include~~] including but not limited to, retraining, suspension, or termination, subject to due process requirements and the employee's collective bargaining agreement.

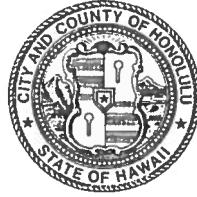
Thank you for the opportunity to provide these comments.

POLICE DEPARTMENT  
CITY AND COUNTY OF HONOLULU

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

**LATE**

KIRK CALDWELL  
MAYOR



SUSAN BALLARD  
CHIEF

JOHN D. MCCARTHY  
CLYDE K. HO  
DEPUTY CHIEFS

OUR REFERENCE WO-KK

February 27, 2020

The Honorable Karl Rhoads, Chair  
and Members  
Committee on Judiciary  
State Senate  
Hawaii State Capitol  
415 South Beretania Street, Room 016  
Honolulu, Hawaii 96813

Dear Chair Rhoads and Members:

SUBJECT: Senate Bill No. 3148, S.D. 1, 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, S.D. 1, 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.

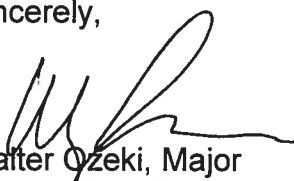
The Honorable Karl Rhoads, Chair  
and Members  
February 27, 2020  
Page 2

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, S.D. 1, Relating to Face Surveillance.

Thank you for the opportunity to testify.

Sincerely,



Walter Ozeki, Major  
Criminal Investigation Division

APPROVED:



---

Susan Ballard  
Chief of Police

Presentation to The  
Committee on Judiciary  
February 27, 2020 10:15 A.M  
State Capitol Conference Room 016

**Testimony in Opposition to SB 3148, SD 1**

TO: The Honorable Karl Rhoads, Chair  
The Honorable Jarrett Keohokalole, Vice Chair  
Members of the Committee

My name is Neal K. Okabayashi, the Executive Director of the Hawaii Bankers Association (HBA). HBA is the trade association representing eight Hawaii banks and two banks from the continent with branches in Hawaii.

The Hawaii Bankers Association is concerned about the bill because the lack of clarity in the definition of “face surveillance”. The vagueness and broadness of the definition of face surveillance may lead to a conclusion that the legally required security cameras in bank branches are considered face surveillance systems. It should be recognized that such security cameras assist law enforcement to identify a perpetrator of a bank robbery. An ATM camera may also be considered face surveillance.

The FDIC requires that banks under its jurisdiction “maintain a camera that records activity in the banking office.” 12 CFR section 326.3.

In consideration of the concerns of the banks, the House Judiciary Committee amended the companion bill, HB 2745, to insert a new subsection which reads as follows:

“(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.”

We ask that the House amendment be inserted into SB 3148, SD 1, with another amendment, which is the deletion of the word “shared”, so the Senate amendment would read as follows:

“(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.

The reason for the deletion of “shared” is that banks do share the video with law enforcement, whether through subpoena, or otherwise. The sharing is a necessity for prevention of crimes.

Thank you for the opportunity to submit this testimony in opposition to SB 3148, SD 1. Please let us know if we can provide further information.

Neal K. Okabayashi  
(808) 524-5161



Hawai'i

**LATE**

Committee: Committee on Judiciary  
Hearing Date/Time: Thursday, February 27, 2020, 10:15 a.m.  
Place: Conference Room 016  
Re: Testimony of the ACLU of Hawai'i in opposition to S.B. 3148, S.D. 1, Relating to Face Surveillance

Dear Chair Rhoads, Vice Chair Keohokalole, and Committee Members:

The American Civil Liberties of Hawai'i ("ACLU of Hawai'i") **opposes** S.B. 3148, S.D. 1 in its current form because, as a result of the most recent amendments, it no longer accomplishes the bill's intent, which is to limit government and private use of facial recognition technology ("FRT").

The ACLU of Hawai'i supports every provision of this bill except for subsection 2(b)—authorizing law enforcement use of FRT for practically any reason—which we request be stricken entirely. Alternatively, the ACLU of Hawai'i proposes that the Committee strike subsections 2(b)(4)-(6) and insert language, below, to ensure that FRT used by law enforcement does not carry racial or gender bias. Amended, S.B. 3148, would safeguard Hawaii's residents against dangerous, invasive, and biased systems that threaten civil rights and safety. **Unamended, the exemptions provided in S.B. 3148, S.D. 1 turn the government use portion of the bill from a prohibition into an endorsement, greenlighting the unfettered use of this technology by law enforcement against the people of Hawai'i.**

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

The recent addition of subsections 2(b)(4)-(6) renders the government use "restriction" in this legislation entirely meaningless and will, if passed into law, **accomplish the opposite of the legislative intent.** 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. Existing use is consistent with what would be allowed under subsections 2(b)(1)-(3)<sup>1</sup> which can lead to prejudicial misidentification and is, alone, problematic.<sup>2</sup> However, the previous committee amended S.B. 3148 to authorize the use of FRT for **practically any law enforcement purpose imaginable, including mass surveillance at demonstrations, enabling police to identify and target political protestors.**

---

<sup>1</sup>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>

<sup>2</sup>The State has determined that current statutes, rules, and regulations prohibit driver's license and ID card photos from being included in the FRT. 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



The costs of this technology to civil rights and liberties substantially and categorically outweigh any benefits. **For this reason, the ACLU of Hawai'i urges the Committee to strike subsection 2(b), which allows law enforcement to use FRT for practically any reason.** If the Committee is inclined to retain parts of subsection 2(b), we ask that, a minimum, the Committee delete subsections 2(b)(4)-(6), which create such broad exemptions as to render the bill's restrictions on government use of FRT meaningless, and that the following language be inserted into the bill to ensure that FRT used by law enforcement pursuant to subsection 2(b)(1)-(3) 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.”

Fourth Amendment and First Amendment rights are at stake, especially for communities of color and women.

Subsections 2(b)(4)-(6) of the bill would authorize law enforcement to use FRT against the protectors at Mauna Kea, if law enforcement simply asserts (whether credibly or not) that there exists a threat of mass violence, that using FRT will protect government facilities and employees, or that use is consistent with the vaguely worded allowance for “future public safety applications.” Further, 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. The exemptions in the S.D. 1 version would allow for FRT to be incorporated into these cameras if done in the name of public safety. The powerful and automated nature of FRT means that law enforcement could track every move a person makes and follow them as they go to work, attend church, go to the doctor, drop their children off at school, attend a political rally, etc. As a result, FRT can have a real chilling effect on people's willingness to engage in civic duties, participate in religious events, or engage in free speech. Abused, this technology can be used on a massive level to target and retaliate against political protestors.<sup>3</sup>

A 2019 study by the National Institute of Standards and Technology found increased rates of inaccuracy in FRT programs when used on women and people of color. Another study, conducted 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. An identification — whether accurate or not — could cost people their freedom or even their lives.

---


<sup>3</sup> Siddiqui and Ulmer, *India's Use of Facial Recognition Tech During Protests Causes Stir*, Reuters (February 17, 2020), <https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ>.

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 Privacy Act,<sup>4</sup> which restricts private use of FRT and is substantially similar to subsection 3 of S.B. 3148, S.D. 1. In light of the highly invasive collection of millions of people's biometric information by private companies,<sup>5</sup> restrictions 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 Hawai'i requests that the Committee amend this measure to prevent the continued, unchecked use of this dangerous and biased technology.

Thank you for the opportunity to testify.

Sincerely,  
  
Mandy Fernandes  
Policy Director  
ACLU of Hawai'i

*The mission of the ACLU of Hawai'i is to protect the fundamental freedoms enshrined in the U.S. and State Constitutions. The ACLU of Hawai'i fulfills this through legislative, litigation, and public education programs statewide. The ACLU of Hawai'i 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 Hawai'i has been serving Hawai'i for 50 years.*

---

<sup>4</sup> 740 ILCS 14, Biometric Information Privacy Act.

<sup>5</sup> 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>.



TESTIMONY OF TINA YAMAKI  
PRESIDENT  
RETAIL MERCHANTS OF HAWAII  
February 27, 2020

**Re: SB 3148 SD1 Relating to Face Surveillance**

Good afternoon Chairperson Rhoads and members of the Senate Committee on Judiciary. I am Tina Yamaki, President of the Retail Merchants of Hawaii and I appreciate this opportunity to testify.

The Retail Merchants of Hawaii (RMH) is a statewide not-for-profit trade organization committed to supporting the retail industry and business in general in Hawaii. The retail industry is one of the largest employers in the state, employing 25% of the labor force.

The Retail Merchants of Hawaii is opposed to **SB 3148 SD1 Relating to Face Surveillance**. This measure limits the government use of face surveillance except under certain circumstances; and limits the private use of face surveillance unless the subject of the face surveillance has given consent.

We feel that this type of legislation is premature as there are a lot of concerns being raised and should be addressed.

Retailers in the last couple of years has seen a rise in organized retail theft. Those participating in organized retail crime range in age from elementary school students to the kapuna. Local companies have lost millions of dollars in the past year alone from shoplifters. With unemployment low, it is difficult to find qualified loss prevention personnel. Retailers rely on surveillance cameras to catch thieves.

This measure would be a big win and help the criminals who admit that shoplifting is their job and that they go to “work” daily - stealing products and items from our stores. With changing technology, surveillance cameras are stating to be able to recognize habitual criminals who enter the store and would be able to alert loss prevention personnel.

Asking a habitual shoplifter their permission to use facial recognition software is not an option. Passing this measure would be in the favor of and just be another win for criminals and a loss for businesses and the community.

We ask you to hold this measure

Mahalo for this opportunity to testify.

**LATE**



**Security Industry Association**

**Testimony Before the Senate Committee on Judiciary  
Hawaii Senate**

**Opposition to Senate Bill 3148**

**Drake Jamali  
SIA Manager of Government Relations  
February 27, 2020  
Honolulu, Hawaii**

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with a bill under consideration by the Committee on Judiciary today, SB 3148, which would severely restrict the use of facial

recognition and facial analysis technology – inaccurately labeled together as “face surveillance” – by both public and private sector entities, affecting their ability to use such technologies for public safety purposes.

The Security Industry Association (SIA) is a nonprofit trade association representing businesses that provide a broad range of security products for government, commercial and residential users in Hawaii and around the US. 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.

Government agencies have made effective use of facial recognition technology for over a decade to improve homeland security, public safety and criminal investigations. A notable success story is the use of the technology to identify and rescue thousands of trafficking victims. In one example last year, a law enforcement officer in California ran across a Facebook post from the National Center for Missing and Exploited Children with a picture of a missing child. The child, who had been victimized for weeks, was successfully recovered after law enforcement ran the photo through one such system, conducting an investigation based on the leads it generated.<sup>1</sup>

Limiting law enforcement use of facial recognition technology only to state booking photographs – as proposed in SB 3148 – would preclude this use described above. Additionally, by banning all non-law enforcement uses, it prohibits other proven public sector uses like protecting employees in their workplaces through secured building access, protecting local infrastructure, and detecting fraud against government programs that aid identity theft and other criminal activity.

Many sectors of the business community are also benefiting from technologically advanced equipment that utilizes biometric identifiers for security purposes, such as authentication, for employee access to buildings or computer networks, and security systems that protect buildings, their occupants and the assets contained therein. For private entities, an exemption to a notification and consent requirement for safety and security uses is essential. A good example is the security provision included in Washington State’s current biometric data law enacted in 2017. This law generally requires notice and consent of an individual before their biometric information is enrolled in a database for commercial use, but provides an express exception where the collection, capture or enrollment and storage of a biometric identifier is in furtherance of a security purpose (RCW 19.375.020, §7). Such an exemption is necessary, because requiring written consent would be unworkable for building systems intended for safety or security applications, as an individual with malicious intent would likely not consent to having their information captured.

The technology can give employers the ability to alert staff and other building occupants of immediate threats to the safety of a building’s occupants, such as where a disgruntled former employee attempts to enter the workplace. Requiring consent would run contrary to ensuring public safety in this case. Without an exception, a consent requirement would essentially preclude using these technologies for the enhancement of access control, intrusion detection, anti-theft, fire alarm, active shooter and other safety and security purposes throughout a building.

Before taking the extreme step of banning certain government applications of the technology and severely restricting others, we urge policymakers to look at sensible transparency measures and clear policies regarding the use of the technology, that could address public concerns without unreasonably restricting tools that have such tremendous public benefits.

---

<sup>1</sup> <https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/>

Unfortunately, the justifications typically cited for banning facial recognition technology are based on several misconceptions. “False positive rates” should not be confused with misidentification. Many facial recognition implementations involve human review as an integral part of a process. The technology is used as a first step in photo comparison that would otherwise be done visually – but there is no automated decision-making in such systems.

Current facial recognition technologies are highly accurate. The National Institute of Standards and Technology (NIST) has found that the facial recognition software is now over 20 times more accurate than it was in 2014, reporting “close to perfect” performance by high-performing algorithms with miss rates averaging 0.1% - reaching the accuracy of fingerprint comparison technology, the identification gold standard.<sup>2</sup> While there will always be error rates for any biometric, consistent performance across all demographic groups is a critical goal for developers to address oft-cited concerns about facial recognition “bias.” We are making significant progress. NIST’s most recent report found “undetectable” differences in performance across demographic groups for the most accurate technologies. To be sure, without this technology we are left with far slower and less accurate processes – with potentially serious safety and security consequences.

For these reasons, we urge you not to advance this bill in its current form and suggest that further examination and multi-stakeholder dialogue on these issues should be undertaken before resorting to such wide-ranging restrictions on a technology that is becoming so critical to public safety.

Sincerely,



Don Erickson  
Chief Executive Officer  
Security Industry Association

Staff contact: Drake Jamali, [djamali@securirtyindustry.org](mailto:djamali@securirtyindustry.org)

---

<sup>2</sup> <https://www.securityindustry.org/report/what-nist-data-shows-about-facial-recognition-and-demographics/>

**SB-3148-SD-1**

Submitted on: 2/22/2020 6:57:53 PM

Testimony for JDC on 2/27/2020 10:15:00 AM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Present at Hearing</b>
Victor K. Ramos	Individual	Oppose	No

Comments:

**SB-3148-SD-1**

Submitted on: 2/24/2020 8:50:54 AM

Testimony for JDC on 2/27/2020 10:15:00 AM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Present at Hearing</b>
Matt	Individual	Oppose	No

Comments:



**SB-3148-SD-1**

Submitted on: 2/25/2020 8:18:12 AM

Testimony for JDC on 2/27/2020 10:15:00 AM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Present at Hearing</b>
Kat Brady	Testifying for Community Alliance on Prisons	Support	Yes

Comments:

**LATE**

**SB-3148-SD-1**

Submitted on: 2/26/2020 10:33:05 AM

Testimony for JDC on 2/27/2020 10:15:00 AM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Present at Hearing</b>
Rayne	Individual	Support	No

Comments:

**LATE**

**SB-3148-SD-1**

Submitted on: 2/26/2020 6:52:18 PM

Testimony for JDC on 2/27/2020 10:15:00 AM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Present at Hearing</b>
Michael W Sawamoto	Individual	Support	No

Comments:

**LATE**

**SB-3148-SD-1**

Submitted on: 2/26/2020 7:15:52 PM

Testimony for JDC on 2/27/2020 10:15:00 AM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Present at Hearing</b>
Nikos Leverenz	Individual	Oppose	No

Comments:

Chair Rhoads, Vice-Chair Keohokalole, and Members:

I am writing in opposition to SB 3148, SD1, based on the amendments taken in the prior committee that afford state and local law enforcement far too much leeway in using unspecified technologies.

It is one thing to grandfather in existing law enforcement uses of a technology that eludes public scrutiny and quite another to lay down far-reaching authority to use it "for other future public safety applications," "for protection of public gatherings where mass violence threats exist," and "for protection of government facilities and employees."

This kind of broad latitude contravenes the intent to protect established individual civil rights and liberties against an emerging technological dragnet that is pervasive in scope and clandestine in operation.

"Other future public safety applications" is entirely conjectural, and it is foolhardy for the Legislature to give a coordinate branch of government statutory carte blanche to do what it will in the future.

Who makes the determination as to whether a public gathering has "mass violence threats," notably far removed from this state's political and social culture? Does any assembly of more than a certain number of persons threaten mass violence?

Regarding the "protection of government facilities," will PSD have summary authority to use facial recognition technology within and around the capitol building as matter of course?

Further, it is incumbent upon this Legislature to set down clear operational parameters on the collection, retention, use, and dissemination of data obtained through this emerging technology and other electronic surveillance tools.

Hawaii is far from alone in not having established regulatory frameworks regarding the proper use of electronic surveillance by law enforcement. That said, it is critical that the Legislature be more proactive in favor of civil liberties and privacy rights given the veil of secrecy that now surrounds the types and uses of current surveillance technologies.

At minimum, there should be independent oversight by multiple parties, including the Legislature, police commissions, and independent citizens commissions, to ensure that established rules are followed in practice. Some jurisdictions also have laws that require written policies, annual impact reports, and approval at public hearings before an agency is even allowed to acquire surveillance equipment and technology.

If civil liberties and privacy rights are to be preserved the public's elected representatives must demand and facilitate more transparency and accountability regarding the retention and use of electronic surveillance equipment and technology, including that related to facial surveillance.

Thank you for the opportunity to provide testimony on this measure.

February 26, 2020

**LATE**

S.B. 3148 Relating to Face Surveillance  
Committee: Senate Committee on Judiciary  
Hearing Date/Time: Thursday, February 27, 2020, 10:15 a.m.  
Place: Conference Room 016, State Capitol, 415 South Beretania Street

Dear Chair Rhoads and members of the Senate Committee on Judiciary:

I write in **support** of S.B. 3148 Relating to Face Surveillance **as originally drafted**.

As a privacy expert, I have worked in the field of data privacy for over 15 years and am a member of the 21st Century Privacy Law Task Force, created by H.C.R. 225 in 2019.

I believe the bill addresses an important area of emerging technology that is in active use by both the public and private sector, but is currently entirely unregulated. In my opinion, the original text of this bill sought to strike the right balance between a citizen's right to privacy in the Hawaii Constitution and the need for public safety and security in an increasingly digital world. This balance is sorely needed while the accuracy of this technology is still being established and while best practices are still being defined for acceptable use.

Unfortunately, the changes made to this bill by the additions in section -2 of line items 2b 4, 5, and 6 no longer strike that balance. They propose allowing mass public surveillance. Although over 20 laws and bills in the US address facial recognition technology, **no other facial recognition law or bill in the US specifically allows mass surveillance, as this bill now does.**

Two countries use facial recognition under the guise of public safety for mass surveillance: **China and Russia**. Most of us are aware that China uses facial recognition to surveil its own citizens; most notoriously during the Hong Kong pro-democracy protests. The country with the second largest facial recognition program is Russia, which is now able to use portable facial recognition equipment in real time at protests similar to the demonstrations of Moscow's municipal elections last summer.

I strongly hope that the Hawaii State Senate continues to align us with other US states and cities on our use of facial recognition, and does not model our methods on those used in China and Russia, and strikes this amendment from the bill.

Thank you for your consideration and the opportunity to support the original text of this legislation.

*Kelly McCanlies*

Kelly McCanlies  
Fellow of Information Privacy, CIPP/US, CIPM, CIPT

