

STATE PRIVACY & SECURITY COALITION

February 7, 2023

Chair Sharon Moriwaki
Vice Chair Chris Lee
Committee on Labor and Technology
Hawaii State Senate
415 South Beretania Street
Honolulu, HI 96817

Re: SB 1085 (Biometrics)

Dear Chair Moriwaki and Vice Chair Lee,

The State Privacy and Security Coalition, a coalition of over 30 companies and five trade associations in the retail, telecom, tech, automotive, and payment card sectors writes in strong opposition to SB 1085, which would decrease consumer safety and significantly impact the state's economy. It is based on an outdated Illinois law, the Biometric Information Privacy Act (BIPA), that was passed in 2008 – less than a year after the smartphone was invented. The abuse of the private right of action (PRA) in the law, as well as the evolution of the online ecosystem, has led to Illinois considering, on a bipartisan basis, how best to reform the statute so as to eliminate the problems that have plagued it since its passage.

Our members recognize the importance of consumer privacy and the sensitivity of biometric data that can be used to identify individuals. However, we caution against replicating the mistakes of BIPA. Specifically, we caution against several provisions of SB 1085, including: 1) failure to recognize the evolution of the modern ecosystem, 2) failure to exempt uses and the provision of biometric data for fraud and security purposes; and 3) the private right of action (PRA).

SB 1085 Does Not Reflect the Modern Online Ecosystem

Because the model this bill emulates was drafted prior to the invention of the smartphone, the bill's requirements do not reflect the evolution of the modern online ecosystem, where consumer-facing entities ("controllers") have very different responsibilities than the entities who process this information on behalf of the consumer-facing entity ("processors"). Processors never interact with a consumer, and yet SB 1085 would require that they obtain consent from the consumer. The practical outcome of this is that the law will impose strict liability on entities who never have an opportunity to obtain consent, but who, for instance, store biometric data or use biometric data to keep consumers safe. In particular, this will affect Hawaii's small businesses in the technology economy who profit from providing services to larger entities.

Additionally, the bill requires written consent, and does not allow for other types of consent. This is not necessarily the easiest or most effective means of gathering consent depending on

STATE PRIVACY & SECURITY COALITION

the context of the situation, and in many cases may be completely unworkable - for example, to members of the disabled community, who may not be able to provide written consent. It also does not account for providing consent or managing consent on devices that do not have screens at all.

The Private Right of Action Will Make Consumers Less Safe

First, including a private right of action for statutory damages would create massive class action litigation exposure for any *alleged* violations of the law by commercial entities, significantly deterring uses of biometric data including for anti-fraud, authentication and other security purposes that benefit consumers. As in Illinois, the result would be to enrich trial lawyers without striking a balance that allows the use of biometric data for purposes that benefit Hawaii residents. Put simply, a private right of action means businesses will be much less likely to offer services that keep Hawaii's consumers' identities safe.

In the last five years, trial lawyers have filed *nearly 1000 class action lawsuits based on BIPA*. 14 years of experience with Illinois' law have shown that this approach leads businesses to decline to offer their full suite of services to state residents, or avoid offering their services in the state at all, due to the overzealous litigation this legislation catalyzed. For this reason, Illinois is considering amending the law in order to address this significant unintended consequence and bring beneficial services back to Illinois consumers.

This is because plaintiff trial lawyers' legal strategy to extract settlements does not rest on the merits of the case, but instead on the opportunity to inflict asymmetrical discovery costs on businesses both small and large – with a cost to defend these frivolous actions averaging \$500,000. These heavy costs to defend cases through summary judgment gives trial lawyers, who bear no or minimal discovery costs, huge negotiating leverage for nuisance settlements, even if the defendant is compliant with the law.

Today, Hawaii has a strong consumer protection statute that the Attorney General can use *right now* to punish bad actors. On the other hand, the PRA in Illinois has not only failed to meaningfully protect consumers, but actually made them less safe, as anti-fraud, convenient authentication, and other beneficial services leave the state because of abusive litigation risk.

SB 1085's Provisions Harm, Rather Than Help, Hawaii Consumers

Using biometric information for security and authentication purposes is a thriving and important sector; biometrics are far more secure and convenient for consumers to use than username/password combinations that come with common knowledge-based questions and answers (“What color was your first car?” “What is your favorite food?”). Tools such as facial recognition and voice authentication are powerful tools to prevent identity theft, cyber crime, and other types of serious fraud.

STATE PRIVACY & SECURITY COALITION

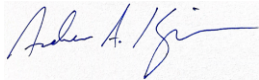
Elderly consumers and disabled consumers increasingly rely on features such as facial recognition to determine who is at their door, and in place of remembering numerous passwords on their computers. The litigation risk that comes along with this statute will mean that these services are far less likely to be offered in the state. Features such as voice recognition in automobiles that prevent distracted driving and help consumers comply with Hawaii's driving laws will likely be unavailable.

Because SB 1085 does not allow for the use of biometric data for security or fraud prevention without written opt-in consent—and does not have a clear security exception—it would put Hawaii residents at great risk of security and fraud threats. Fraudsters, terrorists and other criminals simply will not consent to use of their biometric data for fraud prevention or security, so they would not be able to be screened and logged by private businesses. This is not hyperbole – businesses in Illinois already avoid using biometric data for fraud or security purposes because of the huge class action risk.

It is critical for the safety of consumers that Hawaii not remove an important tool to leverage in combatting cyber threats and preserving secure systems and identities.

To reiterate, SPSC strongly supports consumer protections to ensure that there are appropriate privacy controls and safeguards for data that identifies consumers. We urge this committee to reject a 15-year old law that has never been replicated in another state, and has resulted in the withdrawal of key services and protections for consumers.

Respectfully submitted,



Andrew A. Kingman
Counsel, State Privacy & Security Coalition



February 7, 2023

Senate Committee on Labor and Technology
Hawaii State Capitol
415 South Beretania Street
Honolulu, HI 96813

Re: SB 1085 - Relating to Biometric Information Privacy (Oppose)

Dear Chair Moriwaki and Members of the Senate Committee on Labor and Technology:

On behalf of the Computer & Communications Industry Association (CCIA)¹, I write to respectfully oppose SB 1085, relating to biometric information privacy. CCIA supports the enactment of comprehensive federal privacy legislation to promote a trustworthy information ecosystem characterized by clear and consistent consumer privacy rights and responsibilities for organizations that collect and process data. A uniform federal approach to the protection of consumer privacy throughout the economy is necessary to ensure that businesses have regulatory certainty in meeting their compliance obligations and that consumers are able to exercise their rights. CCIA appreciates, however, that in the absence of baseline federal privacy protections, state lawmakers are attempting to fill in the gaps. To inform these efforts, CCIA produced a set of principles to promote fair and accountable data practices.²

CCIA strongly supports the protection of consumer data and understands that Hawaii residents are rightfully concerned about the proper safeguarding of their biometric data. However, as currently written, SB 1085 goes far beyond protecting such data, which could result in degraded consumer services and experience. We appreciate the committee's consideration of our comments regarding several areas for potential improvement.

1. Overly broad and confusing definitions risk complicating consumers' understanding of their rights and business' compliance efforts.

As currently drafted, SB 1085 includes several overly broad and confusing definitions. For example, "biometric information" should be narrowed to include more specificity around identifying a specific person. CCIA would recommend amending the definition to clarify that it refers to *a specific* individual and not *an individual*. In addition, the definition of "confidential and sensitive information" also invites confusion in so far as the definition groups "social

¹ CCIA is an international, not-for-profit trade association representing small, medium, and large communications and technology firms. For over 50 years, CCIA has promoted open markets, open systems, and open networks. For more information about CCIA please see: <https://www.ccianet.org/about>.

² Computer & Communications Industry Association, *Considerations for State Consumer Privacy Legislation: Principles to Promote Fair and Accountable Data Practices* (January, 2022), <https://www.ccianet.org/wp-content/uploads/2022/02/CCIA-State-Privacy-Principles.pdf>

security number” and “pass code” under this definition. Passcodes inherently pose less risk to a consumer as they are intentionally changeable and not intended to be a unique identifier as a social security number is. CCIA also recommends allowing for more flexibility for organizations, particularly concerning exceptions for security. For example, Washington has approached this by exempting entities that collect and store biometric identifiers in furtherance of a “security purpose.”

2. Sufficient time is needed to allow covered entities to understand and comply with newly established requirements.

As drafted, SB 1085 would go into effect upon its approval. This timeline fails to provide covered entities with a sufficient onramp to achieve compliance. A successful privacy framework should ensure that businesses have an appropriate and reasonable opportunity to clarify the measures that need to be taken to fully comply with new requirements. Recently enacted privacy laws in California, Colorado and Virginia included two-year delays in enforcement of those laws. CCIA recommends that any privacy legislation advanced in Hawaii include a comparable lead time to allow covered entities to come into compliance and would therefore recommend amending the current effective date.

3. Investing enforcement authority with the state attorney general and providing a cure period would be beneficial to consumers and businesses alike.

SB 1085 permits consumers to bring legal action against businesses that have been accused of violating new regulations. By creating a new private right of action, the measure would open the doors of Hawaii’s courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Lawsuits also prove extremely costly and time-intensive – it is foreseeable that these costs would be passed on to individual consumers in Hawaii, disproportionately impacting smaller businesses and startups across the state. Further, every state that has established a comprehensive consumer data privacy law – California, Colorado, Connecticut, Utah and Virginia – has opted to invest enforcement authority with their respective state attorney general. This allows for the leveraging of technical expertise concerning enforcement authority, placing public interest at the forefront.

CCIA recommends that the legislation include a cure period of at least 30 days. This would allow for actors operating in good faith to correct an unknowing or technical violation, reserving formal lawsuits and violation penalties for the bad actors that the bill intends to address. This would also focus the government’s limited resources on enforcing the law’s provisions for those that persist in violations despite being made aware of such alleged violations. Such notice allows consumers to receive injunctive relief, but without the time and expense of bringing a formal suit. Businesses would also be better equipped with the time and resources to address potential privacy changes rather than shifting focus to defending against litigation.

* * * * *



We appreciate your consideration of these comments and stand ready to provide additional information as the legislature considers proposals related to technology policy.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

February 7, 2023

SB 1180 Relating to Biometric Information Privacy
Senate Committee on Labor and Technology
Hearing Date/Time: Wednesday, February 8, 2023, 3:00 PM
Place: Conference Room 224, State Capitol, 415 South Beretania Street

Dear Chair Morikowi, Vice Chair Lee, and members of the Committee:

I write in **SUPPORT** of SB 1085 Relating to Biometric Information Privacy. As a privacy expert, I have worked in data privacy for over 15 years and served on the 21st Century Privacy Law Task Force created by the Legislature in 2019.

Businesses will testify against this privacy legislation, saying it will shut down commerce. And yet other states pass privacy bills and commerce there continues. Illinois, Texas, and Washington have biometric laws very similar to this proposal which passed in 2008, 2009 and 2017, respectively. Commerce continues in each of these states.

This legislation is modeled after the Illinois law; CNN called this law “the gold standard.”¹ I expect the testimony against this bill will specifically rail against the private right of action. Only the Illinois law has this provision and it has been successfully defending the rights of residents of that state since 2008. In 2021, Facebook reached a \$650,000,000 settlement with state residents based off the Illinois law, and Tik Tok reached a \$92,000,000 settlement. The Texas and Washington laws do not have the private right of action and, in spite of being on the books for years, “the laws have hardly been tested”¹. The sad reality is that these laws have made little difference. This is why I support this bill **AS WRITTEN**, including the private right of action.

Thank you for your consideration and the opportunity support this legislation.

Kelly McCanlies

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



CNN “Here’s why tech companies keep paying millions to settle lawsuits in Illinois” Sept. 20, 2022.



1003 Bishop Street
Honolulu, Hawaii 96813
Telephone (808) 525-5877

Alison H. Ueoka
President

TESTIMONY OF ALISON UEOKA

COMMITTEE ON LABOR AND TECHNOLOGY
Senator Sharon Y. Moriwaki, Chair
Senator Chris Lee, Vice Chair

Wednesday, February 8, 2023
3:00 p.m.

SB 1085

Chair Moriwaki, Vice Chair Lee, and members of the Committee on Labor and Technology, my name is Alison Ueoka, President for Hawaii Insurers Council. The Hawaii Insurers Council is a non-profit trade association of property and casualty insurance companies licensed to do business in Hawaii. Member companies underwrite approximately forty percent of all property and casualty insurance premiums in the state.

Hawaii Insurers Council submits comments on this measure. While we support the intent to protect consumers privacy regarding biometric data, we ask for one amendment to the bill. In 2021, the Hawaii Legislature enacted a National Association of Insurance Commissioner's (NAIC) model law on Data Security. This law is specific to the regulation of entities and the data they collect, including biometric records, within and affiliated with the insurance industry. Therefore, we ask that Section -5 be amended to add an exemption to read, "Apply to any licensee that is subject to the Insurance Data Security Law pursuant to Article 3B, Chapter 431."

This language is substantially similar to the provision in SB 1178.

Thank you for the opportunity to testify.



February 8, 2023

The Honorable Sharon Y. Moriwaki
Chair
Committee on Labor and Technology
Hawaii Senate
Honolulu, HI 96813

RE: SIA opposition to SB 1085 Relating to Biometric Data Privacy

Dear Chair Moriwaki, Vice-Chair Lee, and Members of the Senate Committee on Labor and Technology:

On behalf of the Security Industry Association (SIA) and our members, I am writing to express our opposition to SB 1085 under consideration by the committee.

SIA is a nonprofit trade association that represents more than 1300 companies providing a broad range of safety and security-focused products and services in the U.S and throughout Hawaii. Among other sectors, our members include the leading providers of biometric technologies available in the U.S.

Privacy is important to the delivery and operation of many safety and security-enhancing applications of technologies provided by our industry, and our members are committed to protecting personal data, including biometric data.

However, we are concerned that, at a time when many states have now enacted or are considering broader data privacy measures that include protections for biometric data, and the prospect of a federal law setting nationwide data privacy rules draws nearer, SB 1085 is the wrong approach, as it would import an outdated and problematic model from Illinois that is incompatible with the common frameworks that are emerging.

No other state has adopted legislation similar to the Illinois Biometric Information Protection Act (BIPA) of 2008, which has resulted in more harm to consumers and local businesses than any protections. There, businesses have been extorted through abusive “no harm” class actions, and beneficial technologies have been shelved. In fact, many of our member companies that provide products utilizing biometric technologies have chosen not to make these products or specific functions available in Illinois.

Safeguarding biometric information is important, but it should be done in a way that both protects Hawaiians and allows development and use of advanced technologies that benefit them. Beyond opening the door to lawsuit abuse with enforcement through a private right of action and the harm that brings, there are also very real consequences to consumers – including their privacy – for imposing unnecessary limits through overregulation.

For example, biometric technologies play a key role in protecting privacy during transactions that require identity verification, by preventing exposure of personal information (date of birth, Social Security Number, address, etc.) that is far more vulnerable to compromise and abuse.

Biometric technologies create a numerical “template” based on an individual’s biological characteristics to compare with a template or templates already enrolled in a database or on a device. This numerical string of data is readable only within that specific software. Outside and apart from the software and database used to create it, this template by itself does not contain any personally identifiable information. Importantly, it cannot be used to re-create the image (of a fingerprint, face, etc.) that it was derived from. Each provider uses a different process to create and compare templates unique to that particular proprietary software. A template created in one system cannot be used in another.

In this way, the use of mathematical vectors acts as secure cryptography for biometric data, preventing identity hacking even if that data is stolen, and naturally serves to limit unauthorized use by third parties. Most biometric authentication systems store only templates, information that by itself does not put identities at risk if compromised. The collection, storage and processing of this data can easily be optimized to ensure privacy and security using encryption and other cybersecurity and privacy best practices applicable to other forms of personally identifiable information.

We continue to believe that protecting biometric data is best addressed within a broader data privacy framework that protects all types of personal information. Significant changes SB 1085 would be needed to prevent negative impact on Hawaii businesses and consumers. We urge you not to approve the bill in its current form.

Again, we support the overall goal of safeguarding biometric information, and we stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully,



Jake Parker

Senior Director, Government Relations

Security Industry Association

Silver Spring, MD

jparker@securityindustry.org

www.securityindustry.org



February 8, 2023

The Honorable Sharon Moriwaki, Chair
Senate Committee on Labor And Technology
State Capitol - Room 215
415 South Beretania Street
Honolulu, HI 96813

Re: OPPOSE SB 1085 (Lee) - Relating to Biometric Information Privacy.

Chair Moriwaki and members of the Committee:

Thank you for the opportunity to submit testimony for the record regarding SB 1085.

Our corporate partners include companies like Amazon, Apple, Pindrop, and CLEAR, but our partners do not have a vote on or veto over our positions. We urge your committee to **oppose SB 1085**, which would make it prohibitively costly to use biometrics for the safety and security of individuals, and could deny Hawaiians the benefits of rapidly evolving technology.

SB 1085 would effectively ban advanced security measures and routine uses.

Biometrics improve the security of important transactions, electronic devices, and online accounts by assigning a value unique to an individual that cannot be lost, forgotten, faked, or obtained via social engineering. This vastly improves the security of online accounts and phone transactions by eliminating some of the most common ways that hackers and identity thieves access private accounts.

But these security benefits for consumers are threatened because SB 1085's requirements are ill-suited to the online and phone environments. The bill's requirement to obtain "affirmative written consent" and lack of exceptions for security and anti-fraud measures will effectively ban the use of biometrics for security purposes.

For example, an insurance company might analyze a caller's voice to authenticate account ownership. Under this bill, a fraudulent caller who reached the stage where biometric authentication was applied could sue the insurance company for impermissibly analyzing their voice without prior written consent.

The bill's current approach to obtaining "affirmative written consent" also impacts some of the beneficial uses of services backed by biometrics. For example, augmented reality services can make it significantly easier for those with visual or hearing impairments to navigate the world. It might be possible to collect consent from work colleagues to wear glasses that recognize faces and tell the visually impaired person who entered a room, but it might not be possible when attending large conferences or meeting with external groups.

Vague terms and standards could open the door to privacy and security risks for consumers.

We are just at the early stages of exploring how biometric technology can improve our lives, but SB 1085 stands to deny Hawaii residents the choice to take advantage of these advances.

In addition to security benefits, biometric technology benefits consumers in a number of ways. For example:

- Biometrics enable important transactions, such as buying or selling a home, to be conducted remotely—something that has benefited many during the pandemic.
- Biometrics can allow remote unlocking of a car when the keys are locked inside.
- They can offer peace of mind through the ability to monitor one's home while away or to see who is at the door before answering.
- Frequent travelers can speed through the airport security line using biometric verification systems.
- Families with voice-enabled smart home devices can set unique preferences for each family member who can be recognized by voice.

However, a combination of the bill's private right of action that opens the door to frivolous and excessive litigation, as well as vague terms such as "otherwise

profit” and “legally authorized representative” could result in a degradation and outright ban of certain products.

“Otherwise profit”

Section 3(c) states: “No private entity in possession of a biometric identifier or biometric information shall sell, lease, trade, or **otherwise profit** from a person's biometric identifier or biometric information” (emphasis added). One application of this section could either be applied broadly as a prohibition on the use of biometrics as part of a service offered to consumers or as any other part of a for-profit enterprise. Another application could have companies failing to personalize and update their products and services with biometric identifiers for fear of litigation under this section. Finally, another application of this section could have industry interpreting this provision as a de facto prohibition given the high threat of litigation, therefore pulling products and services out of the State of Hawaii.

“Legally authorized representative”

SB 1085 does not provide guidance for companies to authenticate a “legally authorized representative,” increasing the risk of delays to consumer requests or outright fraud. A non-native English speaking customer might want to designate a representative to exercise their rights, but the bill does not lay out the proper forms or authentication required. Even worse, a scammer could pose as an authorized representative to collect vast amounts of sensitive information. Without more guidance as to how to authenticate authorized representatives, companies could be forced to give up information to bad actors.

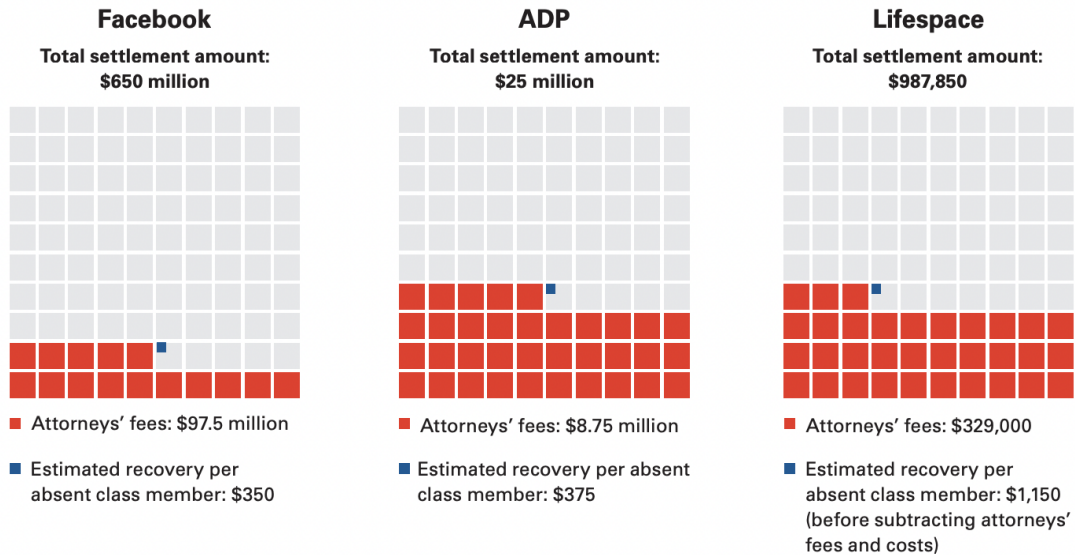
Coupling the bill’s requirements with a private right of action for violations would deter businesses from offering Hawaii’s residents these benefits.

In Illinois, similar legislation to this bill was passed and class action lawsuits subsequently skyrocketed.¹ Unfortunately, those lawsuits primarily benefited trial attorneys rather than individual plaintiffs. The graphic below illustrates in more detail.²

¹ <https://institutelegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf>

² <https://institutelegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf>
progresschamber.org | 1390 Chain Bridge Rd. #A108 | McLean, VA 22101 | info@chamberofprogress.org

Figure 4: Attorneys' Fees as a Proportion of BIPA Settlements²³



These lawsuits also had a chilling effect for consumers: augmented reality products, like face filters, were preemptively blocked for users in the state,³ and some companies opted not to sell their products⁴ in the state at all.⁵

We welcome the opportunity to work with the committee to create alternative legislation that will benefit consumers without denying them the security and convenience biometric technology can provide. For example, allowing a cure period of 30 days would give companies acting in good faith the opportunity to address inadvertent violations without stifling innovation.

Privacy laws and safeguards are crucial to the protection of Hawaii consumers. While we urge the committee to oppose SB 1085, we are happy to be a resource in future efforts to protect consumers' security and privacy without stifling innovation.

Sincerely,

Koustubh "K.J." Bagchi
Senior Director, Technology Policy

³

<https://www.chicagotribune.com/business/ct-biz-meta-pulls-augmented-reality-biometrics-cb-20220518-rp7a6bd7afae5djil24yjy6pgy-story.html>

⁴ <https://support.google.com/googlenest/answer/9268625?hl=en>

⁵ <https://www.sony.com/electronics/support/smart-sports-devices-entertainment-robots/ers-1000/articles/00202844>
progresschamber.org | 1390 Chain Bridge Rd. #A108 | McLean, VA 22101 | info@chamberofprogress.org



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Southwest | Telephone 505.402.5738
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetSW

February 7, 2023

The Honorable Sharon Moriwaki
Chair, Senate Labor and Technology Committee
Hawaii State Capitol
415 South Beretania Street, Room 215
Honolulu, HI 96813

The Honorable Chris Lee
Vice Chair, Senate Labor and Technology Committee
Hawaii State Capitol
415 South Beretania Street, Room 219
Honolulu, HI 96813

RE: SB 1085 – Biometric Information – OPPOSE

Dear Chair Moriwaki, Vice Chair Lee, and Members of the Committee,

TechNet respectfully submits this letter in opposition to SB 1085, relating to biometric information. TechNet's members place a high priority on consumer privacy and as drafted, this bill would create significant hardships for Hawaii employers and could result in stifling important advances in safety and security for consumers.

TechNet is the national, bipartisan network of technology CEOs and senior executives. Our diverse membership includes dynamic American businesses ranging from startups to some of the most recognizable companies in the world. TechNet represents over five million employees and countless customers in the fields of information technology, e-commerce, sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet believes that privacy laws should provide strong safeguards for consumers while allowing the industry to continue to innovate. We understand the Legislature's interest in protecting the data of its constituents, but SB 1085 relies on a flawed model. This bill adopts language from the Illinois Biometric Information Privacy Act (BIPA), a law passed in 2008 that fails to account for over a decade of innovation in technology and business practices. It does not identify and protect against specific privacy harms, instead utilizing a definition of "biometric identifier" that is overbroad and difficult to implement, which, paired with a private right of action, will open Hawaii businesses to costly litigation.

In addition to imposing significant and ongoing compliance costs, this legislation would further burden local businesses with the threat of frivolous class action

litigation. In Illinois, BIPA has been used as a cudgel by class-action law firms seeking large payouts from companies leveraging this technology to benefit consumers, or in many cases from providers of support systems that never even interact with consumers. Illinois has seen over 1,100 class action suits against companies of all types and sizes since 2017. According to the National Law Review, BIPA cases in 2021 “settled in the six-, seven-, eight-, and even nine-figure ranges, even in cases where there have been no allegations that the plaintiffs’ biometric data was hacked or improperly accessed by a nefarious third party. However, the average recovery for a class member is \$440 and attorneys’ fees constitute between 33 to 35 percent of the settlement fund. For example, in a recent settlement, the *maximum* expected payout per successful plaintiff is expected to be \$400, while the law firm that prosecuted the case is expected to receive \$40 million. It should be noted that in the 15 years since BIPA passed, no other state has adopted this model.

SB 1085 will invariably result in some businesses having to remove certain lines of business operations, if not their entire business, from Hawaii not only because of the liability risks illustrated above, but also because it prohibits a private entity from making any profit from a person’s biometric data. There is an important distinction between prohibiting monetization of biometric data unrelated to the business purpose for which the consumer shared that data with a business and, as a practical matter, precluding certain businesses from using that information even upon receipt of affirmative consent by prohibiting them from making any profit from biometric information. This bill does the latter. That places a business in the untenable position of either violating the law subject to significant liability or providing their services and products for free.

The net effect of BIPA in Illinois has been to create a cottage industry of class action law firms and to prevent consumers from accessing pro-consumer, pro-privacy uses of biometric data like products that help provide security through doorbells; prevent identity fraud through use of voice recognition systems; prevent overdoses by way of technology that safely dispenses medicine using biometrics; prevent theft at bank ATMs or securing entire facilities or locations holding sensitive data by way of tools such as fingerprint scanners; help persons with blindness with their surroundings, including by identifying friends and family through use of facial recognition technology; and more.

Hawaii residents and employers deserve privacy protections that safeguard sensitive data while promoting innovation, security, and job creation. TechNet welcomes the opportunity to work with your office to address issues of privacy protection without unintended consequences. Please consider TechNet’s members a resource in this effort.

Thank you for your consideration. If you have any questions regarding TechNet’s opposition to SB 1038, please contact Lia Nitake, Deputy Executive Director, at lnitake@technet.org or 310-940-5506.

Sincerely,

A handwritten signature in black ink, appearing to read "Lia Nitake". The signature is fluid and cursive, with a prominent flourish at the end.

Lia Nitake
Deputy Executive Director for the Southwest
TechNet



Testimony to the Senate Committee on Labor and Technology
Wednesday, February 8, 2023
Conference Room 224

Comments re: SB 1085, Relating to Biometric Information Privacy

To: The Honorable Sharon Moriwaki, Chair
The Honorable Chris Lee, Vice-Chair
Members of the Committee

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League, the local trade association for 47 Hawaii credit unions, representing over 864,000 credit union members across the state.

HCUL offers the following comments regarding SB 1085, Relating to Biometric Information Privacy. This bill would establish standards for the collection, storage, retention, and destruction of biometric identifiers and biometric information by private entities.

While we understand the need for standards with respect to biometric information collection, we would urge caution. Biometrics are currently used on most smartphones, for purposes of logging into different applications, or the phone itself. Most financial institutions with apps for their online services may offer “face ID”, or similar log-in services. These would be considered biometric data.

We understand the need for data privacy legislation, and we prefer a more comprehensive approach to this issue, to avoid possible unintended consequences for our members.

Thank you for the opportunity to provide comments on this issue.



DATE: February 7, 2023

TO: Senator Sharon Moriwaki
Chair, Committee on Labor and Technology

FROM: Mihoko E. Ito

RE: **S.B. 1085 Relating to Privacy**
Hearing Date: February 8, 2023 at 3:00 p.m.
Conference Room 224 & Videoconference

Dear Chair Moriwaki, Vice Chair Lee, and Members of Committee:

We submit this testimony on behalf of the Hawaii Bankers Association (HBA). HBA represents seven Hawai'i banks and one bank from the continent with branches in Hawai'i.

HBA respectfully **opposes** S.B. 1085, Relating to Privacy, which establishes standards for the collection, storage, retention, and destruction of biometric identifiers and biometric information by private entities.

We are concerned that restricting biometric data as proposed in this bill will inhibit legitimate uses of biometric data. With advancements in technology, biometric data has become a secure way for individuals to be identified on smartphones. Many banks have apps to conduct transactions on smartphones, and we would be concerned about legislation that impedes the use of biometrics for the purposes of allowing financial transactions to be secure and to appropriately identify the person performing the transaction. While this particular bill does contain a Gramm Leach Bliely Act (GLBA) exemption, which typically covers certain personal information that is collected by financial institutions, we are still concerned that there still may be unintended consequences that would restrict consumer convenience and security.

Finally, we note that there are more comprehensive privacy proposals that are under consideration before the Legislature, and would suggest that may be a better starting point for discussing privacy policies, rather than approaching elements of privacy like biometrics separately.

For these reasons, we respectfully oppose this measure. Thank you for the opportunity to submit this testimony.

SB-1085

Submitted on: 2/4/2023 10:02:06 AM

Testimony for LBT on 2/8/2023 3:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Caroline Azelski	Individual	Support	Written Testimony Only

Comments:

Support. Thank you

SB-1085

Submitted on: 2/6/2023 2:27:58 AM

Testimony for LBT on 2/8/2023 3:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Robin Miyajima	Individual	Support	Written Testimony Only

Comments:

As someone concerned about data collection and misuse, I support this bill. This information needs to be dealt with properly and securely. After an issue has occurred is too late.