CHAMBER OF PROGRESS

May 22, 2023

Senator Anne Carney, Chair
Joint Committee on Judiciary
Room 438, Cross State Office Building
100 State House Station
Augusta, ME 04333

Representative Matt Moonen
Joint Committee on Judiciary
Room 438, Cross State Office Building
100 State House Station
Augusta, ME 04333

RE: OPPOSE: LD 1705 (Feldman): Commercial Law – Consumer Protection – Biometric Data Privacy

Dear Chair Carney and Chair Moonen,

Thank you for the opportunity to submit testimony for the record regarding LD 1705. On behalf of the Chamber of Progress, a tech industry coalition promoting technology's progressive future, I write to urge you to oppose LD 1705, which imposes unworkable hurdles for businesses trying to use biometric technology to increase security for their customers.

Our organization works to ensure that all Americans benefit from technological leaps. Our corporate partners include companies like Amazon, Apple, and Pindrop, but our partners do not have a vote on or veto over our positions, nor do we speak for our partner companies.

LD 1705's Provisions are Ill-Suited for Modern Applications of Biometric Technology

Biometrics improve the security of important transactions, electronic devices, and online accounts. Biometrics improve security by assigning a value unique to an individual that cannot be lost, forgotten, faked, guessed, written on a Post-It note, 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.

Requirements under LD 1705 are ill-suited to the modern environment and would create hurdles for businesses trying to use biometric technology to increase security for their customers.

The bill's requirement to obtain "affirmative written consent" for use of biometric data makes no provision for, and offers no exceptions for, situations where obtaining such consent would be impossible or impracticable.

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.

While the bill provides an exception to the consent requirement for anti-fraud and security features, the requirement of posting "conspicuous written notice" at every point of collection could still be unworkable. The notice requirement would be impractical, for instance, when a customer was attempting to access account information over the phone and was asked to verify their identity through voice recognition.

Additionally, the bill's requirement that companies return data to consumers upon request, while well-intentioned, runs the risk of exposing sensitive information to hackers. LD 1705 requires any entity in possession of an individual's biometric data to disclose that data and information about its use upon request.

Other state privacy laws, like in California and Colorado, include similar provisions but allow companies to delay their responses in order to address security concerns[1] or merely confirm the data in their possession.[2] These guardrails prevent companies from being forced to turn over data via insecure channels, leaving unique biometric identifiers in email inboxes or cloud accounts, or to turn over sensitive data to fraudsters posing as authorized representatives.

Vague Standards in LD 1705 Create Compliance and Security Risks

[1] https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf
[2] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Additionally, many of the bill's standards are not clearly defined, leaving unanswered questions about how companies should implement consumer protections.

"Strictly necessary" standard creates uncertainty for companies.

The vague standards under the anti-retaliation provisions could create burdensome requirements for companies implementing biometric technology. LD 1705 prevents entities from offering different "levels or quality" of service or charging "different prices" if a consumer declines to consent to use of biometric data. Entities may decline to provide a service to a consumer who withholds consent, but only if the biometric data is "strictly necessary" to the service.

However, how this "strictly necessary" standard would apply remains unclear. For example, if a business takes on additional financial risk when a consumer declines biometric authentication of a transaction, but the consumer still wants to conduct it remotely, would the business allow it?

If biometrics in a product allows speed, convenience, or additional personalization, must businesses re-engineer their products to provide an alternative under the "strictly necessary" standard? Many smart home devices include the option to apply voice recognition to seamlessly switch between settings for different family members.

Without more guidance about how the "strictly necessary" standard applies, companies may be forced to develop equivalent features that can identify different individuals for preference setting without using voice recognition in order to avoid accusations of "conditioning" access on the use of biometrics.

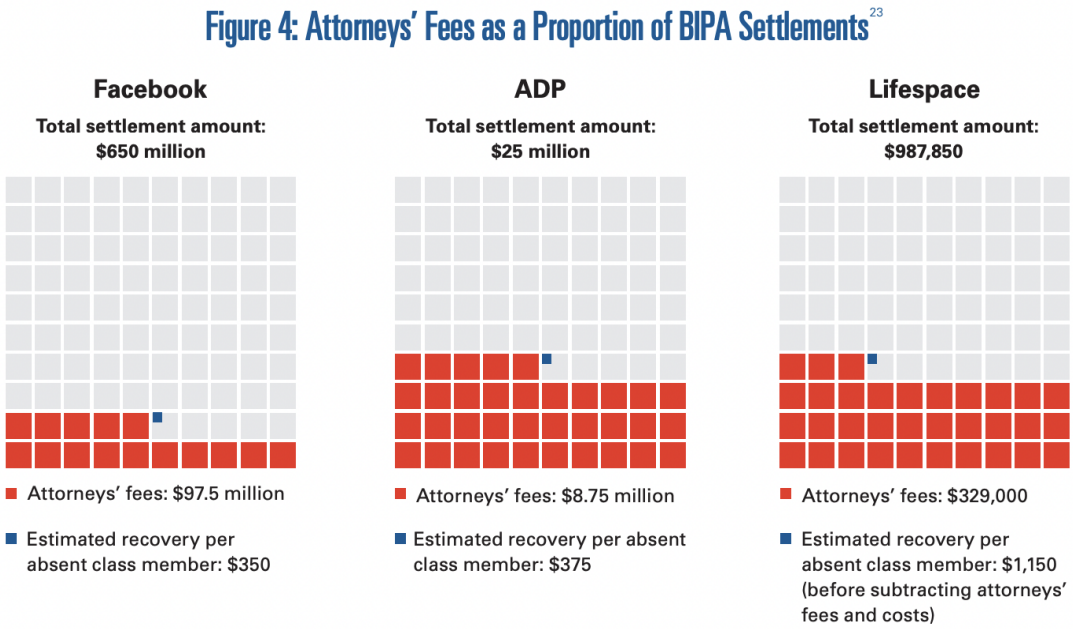
"Authorized legal representatives" needs further clarification.

Additionally, the bill does not provide guidance for companies to authenticate "authorized legal representatives," 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.

Enforcement Mechanisms Could Reduce Options for Consumers

Coupling these vague standards with a private right of action could result in businesses denying access to Maine customers altogether for fear of a lawsuit. For example, similar legislation in Illinois resulted in Google Nest not offering facial recognition services to consumers located within the state.[3]

LD 1705 allows individuals to take private action against companies for violations. This approach is similar to the one followed in Illinois, where class action lawsuits skyrocketed after the passage of the Biometric Information Privacy Act in 2008. Unfortunately, as shown in the graphic below, those lawsuits primarily benefited trial attorneys rather than individual plaintiffs.[4]



These lawsuits had a chilling effect for consumers in Illinois. Augmented reality products, like face filters, were blocked for users in the state,[5] and some companies opted not to sell their products in the state at all.[6] The vague standards in LD 1705 could result in companies opting not to offer their products, like the

[3] https://support.google.com/googlenest/answer/9268625?hl=en
[4] https://instituteforlegalreform.com/wp-content/uploads/2021/10/ILR-BIPA-Briefly-FINAL.pdf
[5] https://www.chicagotribune.com/business/ct-biz-meta-pulls-augmented-reality-biometrics-cb-20220518-rp7a6bd7afae5djil24yjy6pgy-story.html
[6] https://www.sony.com/electronics/support/smart-sports-devices-entertainment-robots/ers-1000/articles/00202844, https://support.google.com/googlenest/answer/9268625?hl=en

popular Amazon Ring or Google Nest, to Maine consumers at all, for fear of inadvertent violations resulting in costly lawsuits.

We welcome the opportunity to work with the committee to create alternative legislation that will benefit consumers without the consequences described above. 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 Maine consumers. We appreciate the author's attempts to protect security and anti-fraud products, but we believe more work needs to be done to avoid unintended consequences for businesses and consumers.

Thank you,

Alain Xiong-Calmes
Director of State and Local Public Policy, Northeast US
Chamber of Progress