STATE PRIVACY AND SECURITY COALITION

January 31, 2019

Senator Kathleen Taylor, Chair
Senate Committee on Workforce
900 Court St. NE, Salem, OR 97301

Committee Members:
Sen. Tim Knopp
Sen. Jeff Golden
Sen. Bill Hansell
Sen. Laurie Monnes Anderson

Re: SB 284 – Biometric Information of Employees

Dear Chairwoman Taylor and Workforce Committee Members,

The State Privacy & Security Coalition, a coalition of 22 media, communications, technology, retail, and payment companies, and six trade associations, writes in opposition to SB 284, prohibiting employers from using employees' biometric data. Very often, our coalition works constructively to help craft state laws that benefit consumers and that are workable for businesses as well. However, SB 284's mandates directly contradict cybersecurity best practices for organizations that must constantly prevent data breaches, malicious hacking, and theft.

First, the definition of "Biometric identifier" goes far beyond any other similar definition in any state statute. It is so broad that its unintended consequences could prohibit, for example, the use of closed circuit security cameras in a warehouse that stores inventory, so that an employer could ensure that no theft or misappropriation of goods is taking place.

Second, the bill would prohibit any professional or semi-professional sports team from using state-of-the-art equipment to monitor its players' health and performance, and ensure that player safety is adequately monitored. It would also eliminate good-natured workplace fitness activities, where daily steps, heart rates, and calories burned are collected and shared in a common space.

Most importantly, however, eliminating the use of biometrics – which significantly constrains the application of multi-factor authentication safeguards – could pose a serious threat to organizational barriers that help prevent unauthorized physical entry into workplaces, as well as preventing hacking and theft of employee data, trade secrets, and sensitive financial and customer data.

In 2016, the California Attorney General's office released its study on data breaches[1] that occurred in and were reported to the state, along with recommendations to businesses as to what constituted reasonable security measures. Malware and hacking, combined with errors by organizational insiders (employees and service providers) constituted 71% of the breaches reported to the state. The report also stated that in the financial sector, the greatest susceptibility to breaches was by employees.

[1] Available at: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

The report's second recommendation was widespread implementation of multi-factor authentication – **it specifically recommends the incorporation of biometrics** to help protect organizational security, and is worth quoting at length:

> The authentication system is failing…[a] stronger form of online authentication uses multiple factors, from independent categories of credentials. Multi-factor authentication pairs "something you know," such as a password or PIN, with "something you have," such as your cellphone or physical one-time-password token, or "something you are," **such as a biometric**, like a fingerprint…Financial institutions have used multi-factor authentication for a decade, sometimes supplementing username and password with biometrics such as "keystroke" dynamics that recognizes a user's unique typing pattern…
>
> This form of authentication should be used by all organizations to help protect access to critical systems and sensitive data…as well as company confidential information like intellectual property and trade secrets.[2]

In an environment where organizations are devoting unprecedented resources to prevent data breaches, and where regulatory authorities are introducing more stringent data security requirements on organizations that own, license, and maintain consumer data, it is unreasonable to eliminate one of employers' most effective tools for preventing, controlling, and remediating data security incidents.

Because this bill's definitions create significant unintended consequences, and the harms this legislation could create in the data security environment far outweigh any benefits it would provide, we strongly urge the committee not to move forward with this legislation.

Respectfully,

Jim Halpert
General Counsel
State Privacy & Security Coalition

[2] Data Breach Report, p. 35