OREGON BUSINESS & INDUSTRY OBI

1149 Court Street NE
Salem, OR 97301

503.580.1964
800.452.7862

oregonbusinessindustry.com
obi@oregonbusinessindustry.com

June 3, 2022

To: Kimberly McCullough, Kate Denison, Office of Attorney General Rosenblum
From: Paloma Sparks, Oregon Business & Industry, Oregon Retail Council
RE: Comments on Consumer Privacy bill draft

Chair and Members of the Committee:

Thank you for the opportunity to submit comments on the latest version of the Attorney General's consumer privacy draft bill on behalf of Oregon Business & Industry and the Oregon Retail Council. OBI is Oregon's most comprehensive business association representing over 1,600 businesses that employ over 250,000 people. The majority of our members are small businesses. We represent multiple sectors across Oregon and serve as the state's Retail and Manufacturing Councils. The Oregon Retail Council is made up of a wide variety of retailers.

We are including redlines and comments on the draft separately, but I will attempt to summarize some of the key comments here. Most importantly, we believe it is essential to make sure any legislation recognizes that not all businesses have extensive resources to implement sweeping changes. Often people hear "corporation" and assume hundreds of staff who can focus just on compliance issues. The truth is that many small businesses have limited staff and need to contract out with attorneys and technical experts to build compliance systems. That reality necessarily takes up a lot of time and is subject to simple human error. We urge you to build some flexibility into the law so that businesses have an opportunity to fix errors before liability attaches.

Section 1: Definitions

The draft bill contains several phrases or concepts that are not defined and we believe they should be clearly defined in this section. In particular, biometric data should be defined here to identify what is and is not included. Without such a definition, many key technological features that customers enjoy will have to be removed from the market due to liability concerns. Additionally, there are some phrases that are more thoroughly defined in section 5, and those should be included here.

For example, it may create confusion that there is a definition of "sale" in section 1 and a different definition for "sale of personal data" in section 5. It makes more sense to transfer over what is in section 5 defining this phrase, including what it does not mean, to section 1. While "targeted advertising" is included in the definitions section, the clarifying language for what it is not is in section 5. We believe it makes more sense to have both in section 1.

An individual reading the bill will naturally refer back to the definitions section to guide their understanding of the bill's intent and terms. We ask that wherever possible key definitions be included in this section.

With regards to a more specific definitions, we believe previous conversations resolved some of our concerns related to the "Definitions" section. For example, it is our understanding that the

definition of “child” will be changed to under 13 as discussed in an earlier task force meeting. There are many circumstances where it makes more sense to allow teenagers more flexibility in how they interact with companies and their sophistication levels to understand privacy implications. There are also several word choices in the current draft that are quite subjective, and we would like to see those changed so all parties understand the expectations under the law.

Additionally, the inclusion of the phrase “or other valuable consideration, or otherwise for a commercial process” in the definition of “sale,” “sell,” “selling,” “sold” will create a great deal of confusion. What is “valuable” or “for a commercial process” is very subjective and open to a wide variety of interpretations. This could confuse the difference between third parties and service providers – even providing data to a service provider, such as a cloud hosting provider, could be considered to be for a ”commercial purpose”. These phrases should be struck to ensure that the meaning is clear for those seeking to understand their rights and obligations.

Section 2: Scope; Exemptions

Within the “Exemptions” section, or in the “Controller Obligations” section as currently written, we urge you to exempt customer loyalty programs. We appreciate the language in the latest draft that states “Nothing in subsection (a) or (b) of this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.” These programs are very important for both retailers and customers and require that customers voluntarily opt-in. These programs provide convenience and discounts that customers rely on. They are fundamentally different from other ways in which customer information is shared with businesses they interact with and should be allowed to continue.

A key element that was included in the draft the task force was working on in 2020 is now missing. That is the broader entity level exemption for financial institutions covered by the Graham-Leach-Bliley Act (GLBA). The current draft will create duplicative and challenging regulations. It also fails to take into account that these types of entities are often interwoven and a single company may be part of a larger entity and all must, necessarily, share data and information to adequately serve their customers. For example, an insurance organization may have separate entities for different lines of insurance while banks may have a traditional banking company and separate trust affiliate or mortgage company, etc. The GLBA requires extensive privacy notifications and generally prohibits disclosure of consumer information without a clear opportunity to opt-out of such information sharing. An entity-level exemption is needed here to ensure that institutions can provide the level of service customers have grown accustomed to. If the entire entity cannot rely on compliance under the GLBA, Oregon customers will likely face a much more complicated and confusing experience when dealing with these institutions and financial institutions will face burdensome and costly compliance for little to no benefit to the institutions or their customers. All recent privacy legislation passed in other states with lone exception of California, have recognized the importance of this by adopting an entity-level exemption for those covered by GLBA. We strongly

urge Oregon to align with the majority of states that have included an entity level GLBA exemption in their comprehensive consumer privacy legislation.

We also ask that the exemption section also state that it does not apply to interactions regulated by the federal Children's Online Privacy Protection Act of 1998, 15 U.S.C. Secs. 6501 to 6506, as amended, *if collected, processed and maintained in compliance with that law or the rules, regulations and exemptions under that law* (emphasis added). This law requires that websites, apps, and online services notify parents and get their express consent before collecting, using, or disclosing personal information from children under 13 if the site is directed at children or has "actual knowledge" that it is collecting information from children. The FTC enforces this law and can impose hefty penalties for violations.

While many stakeholders are submitting language in the "Exceptions" section because that is where it fits best in the current draft, it may make more sense to add a "Limitations" section like other states have done. There are several areas where entities or activities are covered, but the other provisions in the law may have a limited impact on them. Where there are issues that do not neatly fall under an exception or fully covered by the law we urge you to consider if a "Limitations" section may fit the circumstances better.

Section 3: Consumer Rights

The "right to know" language in the Consumer Rights section is troubling. First, no other state has done something like this, which will create huge administrative burdens for businesses that operate nationally. Business relationships with servicers and shippers change all the time out of necessity. This language would require constant updating with likely minimal actual benefit to the customer. Because of the nature of business relationships, the current language could result in inadvertent violations without violating the spirit of the law. There are partnerships that can be formed or changed that result in greater benefit to the customer but if this provision remains it could mean that the customer faces higher costs and longer processing times because of the language creates a disincentive for changing business relationships. It is also unclear how this would work in actual practice.

The language in the "right to opt out" in this section should be specific to solely automated processes. Even where a business attempts to take every precaution, where people are concerned, mistakes will be made. Where processes are solely automated, the risk of error is significantly reduced and ensures consistency in application. Where this language apply to any interaction, human error will almost certainly lead to accidental violations of this provision.

Section 4: Exercising Rights Requests; Responding to Rights Requests

While it certainly seems reasonable to allow third parties to act on behalf of a consumer, this can be abused. Firms and attorneys use this provision to harass businesses. It isn't just technology that consumers use. There are groups that turn this into a cottage industry. The process by which a consumer designates an authorized agent to act on their behalf could be very vague and expansive. We urge for more criteria to be identified for what it means for the consumer and the authorized agent to have a relationship that allows the agent to act on behalf of the consumer.

As states seek to implement their consumer privacy laws, there is a great deal of work still to be done on how to properly comply with opt-out requests. Several states have recognized the practical considerations of this and included the language “if the controller is able to authenticate, with commercially reasonable effort…” We urge a delay in this section to properly develop this in other states and ensure Oregon’s law is applied consistently.

Section 5: Controller Obligations

The inclusion of “willfully disregards” the age of a customer is concerning. Again, we worry about the subjective nature of such a phrase when it comes to understanding the rights and obligations under the law. There must be actual knowledge before an controller is deemed to have willfully disregarded the knowledge that a customer was a child.

We appreciate the exception in subsection (1) that addresses loyalty programs. These are very important programs that are beneficial to customers. Retailers and customers have faced challenges where discrimination clauses are included in privacy legislation that don’t recognize the value of these programs. It is important to understand that loyalty programs and the like, are opt-in programs. Customers must voluntarily enroll and provide information. These programs provide discounts and other benefits that are unique to those enrolled in the program. It is crucial that this language remain in the final version of the bill.

The language in subsection (4)(a)(A)(ii) is concerning, because it may not be possible to operationalize many of the requirements in time. At a minimum, we urge additional time after the effective date to provide sufficient time to develop and adopt technology that will provide a workable tool to allow for this provision to be implementable. The discussion over what this technology might look like is still ongoing in many states and we believe additional time will allow the proper development of this tool. Given the national nature of most businesses and the fact that technology does not stop at the state’s border, it makes sense to ensure that any requirement under this law also work in conjunction with similar requirements in other states.

Customers will likely be engaging with a variety of technologies and opportunities to opt-out or opt-in. Controllers should be able to rely on whichever decision was the most recent in time. For example, a customer may choose to enroll in a universal opt-out technology but then voluntarily opt-in with an individual business. The most recent decision by the consumer should be what controls the obligations that must be met in the business-consumer relationship.

Section 6: Processor Obligations

No comments to provide for this section at this time.

Section 7: Processing De-identified Data

We urge that this section also recognize pseudonymous data, which is distinct from de-identified data. In many cases, the controller will be able to demonstrate that pseudonymous data is kept separate from identifiable data and is subject to effective technical and organizational controls that prevent the controller from accessing such information. It is crucial that the technology of pseudonymizing data be recognized and valued for the protection it provides to consumers.

Section 8: Data Protection Assessments

We urge simplification of the phrasing in subsection (1). The phrase “heightened risk of harm” makes it very challenging to understand what the obligations are under the law. Instead, (1)(a) should state: “A controller shall conduct and document a data protection assessment for each of the following processing activities involving personal data…” Clarity is going to be very important when a controller seeks to implement the requirements under this law.

Section 9: Enforcement

The opportunity to cure is essential. At the end of the day, businesses are operated by people, and they will make mistakes. This will be an incredibly complex law when it is all said and done. There are far too many requirements to presume that any violation is intentional. A controller who is intentionally violating key provisions or the intent of the law will likely ignore this opportunity. The notice should offer a controller the opportunity to cure, not be subject to whether the AG’s office believe a cure is possible. Certainly, controllers will work with the AG to ensure that the cure actually resolves the violation. If the ultimate goal is to protect customers, then remedying the violation certainly meets that intent. We urge that this provision remain, and that the sunset be removed.

It is crucial that this law be enforceable only through AG action. A private right of action subjects all sorts of businesses to frivolous and costly litigation. More often than not, the only winner in those types of cases are the attorneys, not the consumers. We have seen attorneys that simply target certain businesses not based on violations, but on whether the company has the most resources. It becomes a tool of legal harassment. For example, the federal Telecommunications Consumer Protection Act (TCPA) contains a private right of action. Over a period of 17 months, over 3,000 suits were filed, most coming from the same law firms.

These lawsuits don’t capture the worst offenders, just the ones with the ability to pay. The Attorney General has the ability to focus on truly bad actors through targeted action. Of the 18 states that have passed privacy laws since 2018, none have included a private right of action. Even California’s private right of action is very narrow and still has been subject to abuse. We stand ready to work with you to ensure this is a viable enforcement strategy.

Effective Dates

Finally, it is crucial for retailers that the effective date does not fall in January. The holiday season is when most retailers are at their busiest. They simply do not have the ability to focus on serving the bulk of their customer base and implement complex new laws at the same time. We ask that the law go into effect the following July.

Thank you for considering our comments.