

STATE PRIVACY & SECURITY COALITION

March 6, 2023

Chair Floyd Prozanski
Vice Chair Kim Thatcher
Senate Judiciary Committee
Oregon State Capitol
900 Court Street NE
Salem, OR 97301

Re: SB 619 (Comprehensive Privacy)

Dear Chair Prozanski, Vice Chair Thatcher, and Members of the Committee,

The State Privacy & Security Coalition, a coalition of over 30 companies and six trade associations in the telecom, retail, technology, automotive, payment card, and health care sectors, writes in opposition to SB 619, with the hope that continued work will allow us to remove our opposition.

As an “inner table” member of the Attorney General’s Privacy Task Force for the past two-and-a-half years, we would like to commend the work of the Attorney General and her tireless staff, who have met with stakeholders regularly and have moved the process forward in a substantive, productive manner.

Unfortunately, the draft before us today still deviates from other state privacy laws in ways that do not appropriately balance increased control and transparency for consumers over their data with operational workability for businesses. Our hope is that continued discussions can bring us to this balance, but at the moment, the bill still needs significant work. We look forward to working with this committee as well as the Attorney General’s office to get there.

Enforcement

The enforcement structure remains a significant issue, as the bill currently contains a private right of action, a notice-and-cure period that is discretionary and that sunsets only one year after the law goes into effect, and individual liability, which would mean that executives, employees, and others could be held personally liable for certain violations. No other enacted comprehensive privacy statute includes such provisions. Until enforcement moves to Attorney General-exclusive enforcement with a meaningful right to cure and the individual liability is removed, SPSC must continue to oppose this legislation.

Global Opt-Out

While we do not object to Oregon including requirements for a global opt-out mechanism to be implemented, there are significant issues with the way this is drafted currently. First, the global opt-out currently covers not just opting out of sale or targeted advertising, but would mandate opting consumers out of profiling as well. The problem with this is that such an opt-out mechanism does not yet exist. Currently, tools are being built to comply with California’s and

STATE PRIVACY & SECURITY COALITION

Colorado's statute and regulations, but these tools do not contemplate profiling. It is literally impossible to provide a universal opt-out mechanism for profiling at this moment.

Additionally, the provisions do not consider important issues such as the disclosures that opt-out developers make to consumers (ensuring that they do not over-promise or constitute dark patterns), requiring developers to authenticate the user's residency (as it will not be possible for controllers to do so using the universal opt-out mechanism), how the data security responsibilities are allocated between the parties, and the time required to implement technical solutions required by the law.

While these issues are complex, one way to solve this would be to include a provision of reciprocity so that controllers who comply with other states' regulations are deemed to be in compliance with Oregon's rules. We would be happy to work on these provisions but they are critical to get right given that this technology is nascent and has yet to be implemented by the vast majority of businesses.

Inclusion of "Households" and "Devices" In Statutory Thresholds

The bill currently would include both devices and households to determine whether controllers are subject to this act. However, this not only needlessly confuses the matter and blurs the bright-line test that exists in other comprehensive privacy laws of a clear number of consumers from whom the controller collects personal data.

Additionally, including these concepts dramatically lowers the threshold, bringing in small businesses who likely are not planning on being affected by the bill. A recent study by Deloitte found that the average household contains 22 *connected devices*.¹ The inclusion of devices could effectively cut the threshold from 100,000 consumers to nearly 5,000 based on this data. We recommend aligning this with other state privacy laws to retain clarity.

Portability Right

This right needs to be cabined to data *provided by the consumer to the controller*. Otherwise, it risks opening significant issues of competition among controllers.

Again, this is the standard in other enacted comprehensive privacy bills, and we believe this is an area where alignment is key.

Disclosures

The bill significantly deviates from other state privacy laws by requiring a level of detail in required disclosures that could compromise security and impose unreasonable compliance costs on controllers and processors alike.

¹ <https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/connectivity-and-mobile-trends.html>

STATE PRIVACY & SECURITY COALITION

The prime example of this is the bill requirement for a controller to disclose to the consumer of “specific third parties” to which the controller has disclosed the consumer’s personal information. This obligation raises serious security concerns – forcing controllers to disclose details about data flows that could be valuable in the hands of bad actors. It would also burden small and large businesses alike by requiring the creation and adoption of internal technology and software functionality to track data flows with a level of granularity that does not exist currently. Perhaps even more concerning, such a requirement risks violating trade secret laws as well as forcing businesses to violate terms of individual customer contracts by requiring disclosure of individual customer names and proprietary information.

Conversely, disclosing *categories* of third parties provides consumers with a meaningful way of understanding the wide range of uses for which consumer data can be shared, including financial, cyber and risk mitigation services without risking security and without the overwhelming costs and operational burden to controllers.

Biometric Data Definition

Again, this critical definition currently deviates significantly from all other enacted state privacy laws, because it is unacceptably broad. This definition is intended to cover data that *actually identifies* an individual – not that *could identify* one. This definition is closer to the Illinois Biometric Privacy Act (BIPA) definition that has caused massive levels of confusion regarding what biometric data is.

We would request that this definition be altered to match with the definition used by other state privacy laws.

Children’s and Teen Privacy

This bill deviates not only from other state privacy laws in its requirements for children’s and teen data, but also deviates troublingly from the standard of knowledge in the Children’s Online Privacy Protection Act (COPPA). By introducing a “constructive knowledge” standard, businesses will likely be incentivized to collect additional information from users to verify age – something that many businesses and consumer advocates alike believe is ultimately harmful to children and teens.

We request that the bill move to an “actual knowledge” standard and additionally conform the parental consent and advertising provisions to other state laws’ requirements. This is critical for interoperability.

Profiling

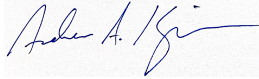
The scope of the profiling opt-out right should be narrowed, consistent with approaches in Connecticut and Colorado, which clearly carve out higher-risk profiling based on automated processing with human review. Focusing the profiling opt-out right on “solely” automated profiling is the best approach to protecting consumers against potential harms, while still encouraging and facilitating the vast benefits of automated processing for Oregon residents.

STATE PRIVACY & SECURITY COALITION

* * *

In addition to the key issues listed above, we have other concerns including definitional scope issues., We hope to continue working with stakeholders to get SB 619 to strike that balance of increased consumer control and transparency, and operational workability.

Respectfully submitted.



Andrew A. Kingman
Counsel, State Privacy & Security Coalition