STATE PRIVACY & SECURITY COALITION

February 7, 2026

The Honorable Floyd Prozanski, Chair
The Honorable Kim Thatcher, Vice Chair
Senate Committee On Judiciary
Oregon State Legislature
900 Court St. NE
Salem, Oregon 97301

RE: SB 1587 – Relating to Data Brokers

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

The State Privacy & Security Coalition (SPSC), a coalition of more than 30 companies and seven trade associations across the retail, technology, telecommunications, payment card, and healthcare sectors, appreciates the opportunity to provide testimony on Senate Bill 1587.

We understand the sponsor's concern regarding the misuse of personal data in ways that may expose individuals, including immigrant communities, to harm. We share that concern and agree that certain categories of personal data merit heightened protections. Our coalition has long supported targeted safeguards to address such concerns, including through participation in the Attorney General's privacy task force and work last session to advance amendments prohibiting the sale of precise geolocation data and children's data. Each of those efforts reflected a shared commitment to protecting vulnerable individuals through policy that is clear, targeted, and enforceable, while preserving consistency and workability across Oregon's privacy framework.

We approach SB 1587 in that same spirit. As drafted, however, the bill adopts an approach that is broader and less precise than necessary to address the specific harms motivating the legislation. The resulting ambiguity and overbreadth risk weakening Oregon's privacy framework rather than strengthening protections for individuals most at risk.

I. SB 1587 LACKS CORE OPERATIVE DEFINITIONS NECESSARY FOR COMPLIANCE AND ENFORCEMENT

Effective privacy laws depend on clear statutory boundaries. SB 1587, however, relies on undefined terms such as "sell" and "otherwise provide" to establish the scope of its central prohibition. In the absence of clear definitions, regulated entities are left to infer which data transfers the Legislature intends to restrict.

The absence of a definition for "sell" creates immediate uncertainty. Common practices such as data transfers for a service fee, data sharing between affiliated entities, or disclosures to vendors acting on behalf of a business could each be treated as a sale, even though those arrangements are routine and widely accepted in privacy frameworks. Likewise, the phrase

"otherwise provide" is overbroad. Without limiting language, the term could encompass routine and legally required disclosures, including sharing data with fraud prevention or cybersecurity partners, responding to subpoenas, or fulfilling consumer access and portability requests. Each activity could trigger liability solely because the statute fails to draw a clear line between permissible use and prohibited conduct.

Oregon's comprehensive privacy law avoided these problems by defining its core terms and clearly identifying permissible data transfers. SB 1587 would benefit from the same precision, including definitions aligned with existing privacy frameworks and explicit recognition of lawful disclosures that serve legitimate consumer and public interests.

II. THE BILL'S CORE PROHIBITION IS OVERBROAD AND DIFFICULT TO APPLY IN PRACTICE

Section 1(2) of SB 1587 prohibits a data broker from providing brokered personal data if the broker has "reason to believe" the recipient will use the data, directly or indirectly, for purposes related to enforcement of civil law. While intended to prevent misuse, the provision relies on a series of undefined and expansive terms that make compliance impracticable.

- **Reason to believe.** The standard imposes a subjective and forward-looking obligation that requires data brokers to predict how a recipient might use data in the future, even when the broker lacks visibility into downstream operations or the ability to monitor subsequent use. Liability may therefore turn on hindsight rather than on facts known at the time of disclosure.

- **Use.** The bill does not define what it means to "use" data. Without limits, the term could encompass routine activities such as storage, analysis, internal review, or incidental access, sweeping in ordinary and socially beneficial functions like compliance monitoring and customer support.

- **Directly or indirectly.** This language extends potential liability to downstream actions beyond a broker's knowledge or control, including later disclosures or internal uses by third parties that were neither authorized nor reasonably foreseeable.

- **Purposes related to enforcement of civil law.** Civil law enforcement is a broad category that includes regulatory compliance, internal investigations, audits, and litigation defense. Each of these activities relies on established legal processes and serves legitimate public and private interests.

Accordingly, these elements create a prohibition that is difficult to interpret and nearly impossible to apply with confidence. The likely result is a chilling effect on lawful data sharing, as brokers err on the side of withholding information to avoid inadvertent violations, undermining compliance, security, and consumer-serving operations without delivering meaningful privacy benefits.

III. SB 1587 EXPANDS PRIVATE ENFORCEMENT IN WAYS UNTETHERED TO CONSUMER HARM

SB 1587 creates a private enforcement regime that departs from Oregon's existing privacy framework and is not tied to consumer harm. Under current law, the Attorney General serves as the primary enforcer of privacy obligations, promoting consistent application and focusing enforcement on conduct that causes real injury. SB 1587 instead allows any individual to bring a civil action whenever data is provided in violation of the statute, even where no misuse of data, tangible injury, or causal connection is alleged. The bill also authorizes any person, not only affected individuals, to seek injunctive relief. That structure significantly expands exposure and increases the risk of duplicative or conflicting court orders, particularly given the statute's ambiguous substantive standards.

Experience in other jurisdictions shows that open-ended private rights of action often result in opportunistic litigation, inconsistent judicial interpretation, and increased compliance costs, with limited corresponding benefit to consumers. Oregon's comprehensive privacy law deliberately avoided those outcomes by reserving enforcement authority to the Attorney General. Aligning SB 1587 with that model would preserve accountability while reinforcing clarity and predictability in Oregon's privacy framework.

* * *

We commend the Legislature's continued leadership on privacy and data protection and respect the concerns SB 1587 seeks to address. As drafted, however, the bill's lack of clear definitions, expansive and indeterminate prohibition, and broad private enforcement provisions introduce substantial legal uncertainty without a corresponding increase in consumer protection.

We remain eager to work with the sponsor and the Committee to develop a solution that addresses those concerns while maintaining clarity, proportionality, and consistency with Oregon's existing privacy framework. We would welcome the opportunity to discuss these issues further.

Respectfully submitted,

Andrew A. Kingman
Counsel, State Privacy & Security Coalition

William C. Martinez
Counsel, State Privacy & Security Coalition