STATE PRIVACY & SECURITY COALITION

February 9, 2021

Oppose House Bill 1330
House Industry, Business and Labor
Chairman Mike Lefor

Dear Chairman Lefor and Members of the House Industry, Business and Labor Committee,

The State Privacy and Security Coalition, a coalition of 29 leading telecommunications, technology, retail, payment card, automobile, and online security companies, as well as seven trade associations, writes in opposition to HB 1330. The bill contains a blanket opt-in provision that will frustrate consumers, does not define key terms (and confusingly defines others), and is not interoperable with other state privacy laws. The inclusion of a Private Right of Action, instead of AG enforcement, would contradict other omnibus consumer privacy laws' enforcement provisions and lead to a torrent of frivolous class action litigation.

Importantly, we note that this state's legislature commissioned a comprehensive legislative interim study of data privacy, and concluded after significant deliberation that this was not the right time to attempt this sort of complex regulation at a statewide level. We would urge the legislature to follow this recommendation and not advance HB 1330.

Opt-In Framework

This bill goes far beyond what the Federal Trade Commission's Privacy Framework recommends companies implement. The Framework recognizes that opt-in consent is very important to provide in cases where companies may be handling sensitive data (e.g., health information or precise geolocation information), but that generally, consumers should be given choices within the context of the transaction, because it helps them understand what they are assenting to or opting out of.

The requirements in this bill would inundate consumers with notices that, in practical terms, would create unnecessary burdens for the ordinary course of business for transactions that have no impact on a consumer's privacy. What happens if a company changes cloud storage providers and consumers do not consent? What happens if a business changes payroll processors and an employee doesn't consent?

Even many privacy advocates oppose opt-in consent provisions such as this, because the consumers lose the ability to distinguish between what decisions about their data require extra attention and what decisions are routine operational transactions.

Finally, many of the data elements – such as professional history and residence details - listed in the definition of "protected data" are publicly available. Exemptions for publicly available information are found in nearly every privacy law in the nation, and this is a concept supported by the FTC framework.

Private Right of Action

The data shows that private rights of action – with their inevitable class action lawsuits - are not effective remedies for consumers. In a study[1] of consumer federal class action matters filed in the Northern District of Illinois from 2010-12, researchers concluded that "the cost of using the consumer

[1] *High Cost, Little Compensation, No Harm to Deter: New Evidence on Class Actions Under Federal Consumer Protection Statutes*, Columbia Business Law Review (2017).

class-action procedural device to compensate such a small fraction of consumer class members outweighs the aggregate amount delivered as compensation to consumers." Moreover, "the aggregate amount that class members typically receive comprises a small fraction of the nominal or stated settlement amount. Since courts base attorneys' fees on [this amount]…***attorneys' fees often equal 300%-400% of the actual aggregate class recovery***." (emphasis added). The study concluded that "the findings here confirm the view that class-action settlements are more effective in transferring money from the defendant to class counsel than in compensating class members."

Definitions

- **"Covered Entity":** the definition of "covered entity" would apply to any legal entity in the state, meaning that these new regulations would saddle small businesses with the same costs as larger businesses. Combined with the omitted and unclear definitions we identify below, this would have a significantly negative effect on the state's small businesses. In a post-COVID-19 landscape, we believe that the priority should be on resuscitating the state economy, not imposing additional compliance costs on businesses.
- **"Protected Data":** This definition is not found anywhere else in any state law in the nation. One of the hallmarks of state privacy legislation is the need for interoperability, ensuring that as much as possible, entities that conduct business across state lines are able to implement similar rules. This definition is not tied to any of the major frameworks that exist in other states, and is both overinclusive (for instance, the number of followers someone has is not particularly sensitive) and underinclusive (excluding other types of data that could be reasonably linkable to consumers). Additionally, the definition includes data elements that, for many companies or in many uses, would be covered by existing federal laws such as the Fair Credit Reporting Act.
- **"User":** This definition does not confine the scope of the bill to North Dakota residents. This would raise immediate dormant commerce clause issues upon passage, raising doubts about whether the bill would be enforceable at all.
- **"Opt-In," "Sale,"** and **"Collect":** These are two critical terms in the bill, as they determine the scope of information covered, the activities prohibited, and the type of transfers regulated. However, they are not defined and as such, would likely create dramatically different interpretations among businesses, which would lead to inconsistent application of the bill and ultimately, significant consumer confusion.

We request that HB 1330 not advance. We believe that it is inconsistent with national data privacy standards, would frustrate consumers, and is in fact inconsistent with this legislature's own conclusions just six months ago.

Respectfully submitted,

Andrew A. Kingman
General Counsel
State Privacy and Security Coalition