STATE PRIVACY AND SECURITY COALITION

April 3, 2018

Chairman Kevin Meyer
Senate State Affairs Committee
State Capitol Room 103
Juneau AK, 99801

Re: AK SB 118, the "Right to Know" Act

Dear Chairman Meyer and Members of the Committee,

The State Privacy and Security Coalition, a coalition of 23 leading communications, technology, retail, and media companies and six trade associations, opposes Alaska SB 118, the Right-to-Know Act. For the reasons discussed herein, the bill would actually be detrimental to consumers and would create a very costly compliance burden for businesses, thereby discouraging investment in the State. It would create a strong incentive for companies to make all data that they disclose individually identifiable in order to be able comply with the law (a move that could harm consumers rather than helping them), and would impose needless legal expense with minimal public benefit. Finally, the bill is unnecessary – nearly every business with a website voluntarily discloses what types of information it collects and how it shares that information in its online privacy policy.

It is important to understand that that the Right-to-Know Act would be a total outlier with requirements that go far beyond any federal or state law, and would actually make consumers more identifiable, because the bill requires companies to not only begin keeping consumer information in a form that will be linkable and identifiable, but to sort through current customer information and make it identifiable. This requirement is not an incidental part the bill – requiring accountings of information that is not identified is the bill's central tenet. It would undermine consumer privacy by creating strong disincentives against companies for taking the pro-privacy step of keeping data in a form that very likely does not identify individuals, but might theoretically be "capable of" re-identification.

Moreover, businesses (even many small businesses) in the state would have to hire lawyers to decipher its complex requirements and then spend huge sums of money tracing disclosures of information that may not actually identify an individual.

It would also divert significant IT resources away from initiatives that advance innovation or cybersecurity, instead putting those resources towards extensive legal and technical compliance measures to avoid enforcement risk.

Under California's much more workable "Shine the Light" law (Cal. Civ. Code § 1798.83), which has been in operation for more than 15 years, our members have established compliance

systems but typically receive only a handful of legitimate requests each year regarding disclosures of personally identifying information to third parties for marketing purposes. Many of the requests received are actually fraudulent requests for information, including spam, fraud, or phishing attempts. Because of enforcement risk under the bill, businesses would be forced to address all of the fraudulent requests, which requires re-identifying de-identified data in an attempt to confirm that the people making the requests are who they say they are.

Although the bill says that it applies to the defined term "customers," nowhere does this legislation limit its reach to Alaskan residents, encompassing anyone who uses the internet who provides a sweeping range of non-personally identifying information to a business. This means the bill would reach every website or other service to which a person connects with a device, whether for business purposes or as a consumer. In many cases, businesses will not even have name and address information for these "customers" to be able to authenticate them and tie them to disclosures, but must somehow furnish an accounting of all businesses that received non-identifiable or identifiable information about the "customer" from the business.

We further caution against attempting to mandate particular forms of notice or to require placing privacy disclosures and statements of consumers' rights in online terms of use (as this bill would require). Indeed, these kinds of laws and enforcement criteria effectively require businesses to provide lengthy disclosures - which consumers are less likely to read -- in order to avoid costly enforcement actions.

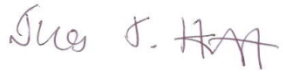
The private right of action contained in the bill compounds the problems the bill would create. The vague and far-ranging requirements of this bill mean that a business could, for example, be found in violation of the statute if it failed to disclose that it had shared how many of its uses have college degrees with a marketer, while knowing no other information about the individuals. This is an invitation to an explosion of class-action litigation that will make lawyers happy and consumers less safe. Again, the bill's insistence on requiring shared data to be identifiable puts all Alaskan residents at risk.

Increased consumer transparency can be achieved without legislative mandates such as these. Furthermore, important progress has already been made on consumer transparency through self-regulatory efforts, such as the National Telecommunications and Information Administration ("NTIA") multi-stakeholder process, which created an FTC-enforceable code of conduct on mobile application transparency for participating companies.

Our coalition members recognize that privacy is very important and vigilantly and proactively working to keep users, subscribers, and customers safe. While this bill does not accomplish that objective, we would be happy to discuss best practices for data security at your convenience.

For the foregoing reasons, we respectfully request that AK SB118 be withdrawn.

Sincerely,



Jim Halpert
Counsel, State Privacy & Security Coalition