

STATE PRIVACY & SECURITY COALITION

October 11, 2023

Senator Anne Carney
Chair, Committee on Judiciary
Room 438, State House
Augusta, ME 04333

Representative Matt Moonen
Chair, Committee on Judiciary
Room 438, State House
Augusta, ME 04333

Re: LD 1977 (Consumer Privacy) - Oppose

Dear Chair Carney, Chair Moonen, and Members of the Committee,

The State Privacy and Security Coalition, a coalition of over 30 companies in the retail, telecom, tech, automotive, and payment card sectors, as well as six trade associations, writes in strong opposition to LD 1977, which is neither interoperable with the 12 other states which have adopted comprehensive privacy laws, nor will meaningfully advance consumer privacy. LD 1997 appears to attempt combining comprehensive privacy with algorithmic discrimination, children's privacy, data broker registration, and social media regulation. As we discuss below, the result is that the bill is extremely confusing, and would burden Maine businesses with tens of millions of dollars in compliance costs. Specifically, we caution against several provisions of LD 1977, including: 1) the private right of action (PRA), 2) opt-in consent provisions pertaining to covered data and sensitive data, and 3) impact assessment requirements for uses of covered algorithms.

As we have advocated consistently over the past two legislative sessions, we believe the best path forward is the bipartisan framework that has been vetted by numerous task forces, working groups, and state legislatures. The framework pioneered by Washington State and ultimately adopted by Connecticut, Colorado, Oregon, Delaware, Virginia, Indiana, Montana, Texas, Iowa, Utah, and Tennessee provides consumers with strong consumer rights and serious internal and external obligations for businesses.

Put simply: there is a clear state privacy template that now covers nearly 25% of the US population, and LD 1977 diverges so significantly from this template that it would isolate Maine's economy without providing those same protections for consumers.

While LD 1973 itself needs several important changes, it is much closer to the template referenced above, and should be the vehicle for consumer privacy moving forward in this session.

STATE PRIVACY & SECURITY COALITION

The Private Right of Action Will Make Consumers Less Safe

First, including a private right of action for statutory damages could create massive class action litigation exposure for any *alleged* violations of the law – even technical and unintentional violations - by commercial entities, significantly reducing the services offered to consumers and creating a cottage industry of frivolous litigation. We have seen this take place in Illinois under the Biometric Information Privacy Statute (*BIPA*).

Far from a hypothetical, the litigation numbers elsewhere bear this out: in the last five years, trial lawyers have filed *more than 1000 class action lawsuits based on BIPA*. 14 years of experience with Illinois' law have shown that this approach leads businesses to decline to offer their full suite of services to state residents, or avoid offering their services in the state at all, due to the overzealous litigation this legislation catalyzed. For this reason, Illinois is considering amending the law in order to address this significant unintended consequence and bring beneficial services back to Illinois consumers.

This is because plaintiff trial lawyers' legal strategy to extract settlements does not rest on the merits of the case, but instead on the opportunity to inflict asymmetrical discovery costs on businesses both small and large – with a cost to defend these frivolous actions averaging \$500,000. These heavy costs to defend cases through summary judgment gives trial lawyers, who bear no or minimal discovery costs, huge negotiating leverage to extract nuisance settlements, even if the defendant is compliant with the law or the violation did not result in consumer harm.

Furthermore, studies have revealed that private rights of action fail to compensate consumers *even when a violation has been shown*, and instead primarily benefit the plaintiff's bar by creating a "sue and settle" environment.¹ This is not to say that Maine lacks effective enforcement options outside the trial bar – to the contrary, it has a strong consumer protection statute that the Attorney General can use *right now* to punish bad actors. On the other hand, the PRA in Illinois has not only failed to meaningfully protect consumers, but actually made them less safe, as anti-fraud, convenient authentication, and other beneficial services leave the state because of abusive litigation risk.

LD 1977 Is Too Confusing to Ensure Effective Compliance

Even in the categories of for-profit businesses it attempts to regulate, LD 1977 fails the most basic threshold for compliance: clarity by those reading and interpreting it. This will not only deter compliance but further encourage litigation under the private right of action.

In contrast to the easily understandable categories of LD 1973 (controller, processor, third party), LD 1977 sets forth numerous categories of businesses, some of which appear to overlap,

¹ Mark Brennan et al., *Ill-Suited: Private Rights of Action and Privacy Claims*, U.S. Chamber Institute for Legal Reform (July 2019).

STATE PRIVACY & SECURITY COALITION

so that a business could be, for instance, both a “Covered entity” and a “covered high-impact social media company,” as well as a “large data holder.” To wit, a business must determine if it is a:

- Covered Entity
- Covered High-Impact Social Media Company
- Data Broker
- Large Data Holder
- Service Provider
- Small Business
- Third Party

Similarly, this bill significantly departs from the conventional delineations of the types of data, which comprise: 1) personal data (the data that is regulated by this legislation); 2) sensitive data (a subset of personal data that receives heightened protections) 3) deidentified data (exempt); and 4) pseudonymous data (partly regulated by this legislation). Instead, LD 1977 creates its own unique terms, and creates ambiguity around threshold issues such as “what happens to data that is transferred from a covered entity to a service provider – is it covered data still or is it service provider data, and as such no longer constrained by the covered data prohibitions?”

Even as it is overbroad, it is lacking key definitions. The term “transfer” is used 111 times in the bill but is not defined. There is no definition of “consumer” or “user,” raising significant dormant commerce clause issues.

The bill states that it exempts state agencies and entities that provide data to those state agencies, but includes in the definition of “service provider data” data that entities provide to state agencies; again, creating significant compliance confusion and liability issues.

LD 1977 Inverts the Structure of Comprehensive Privacy Laws and Departs from FTC Guidance, Which Would Further Isolate Maine Businesses and Consumers

Critically, LD 1977 ***completely inverts*** the structure of other comprehensive privacy laws and departs from FTC guidance regarding the centrality of first-party advertising.

First, the bill inverts the structure of other comprehensive privacy laws by *permitting only those uses which are exceptions in other laws*. Those laws set forth clear consumer rights, and require consent when entities use data beyond what was initially disclosed to the consumer or when processing sensitive data. They then set forth permissible internal uses that are outside the scope of the bill’s mandates. LD 1977 inverts this structure by permitting *only those activities that are excepted in other statutes*.

Additionally, the bill would require consent for first-party advertising, which contravenes the best practices established by the Federal Trade Commission. The FTC has stated that there are

STATE PRIVACY & SECURITY COALITION

everyday uses – including first-party advertising – that do not require consent, but that there are additional types of data processing, such as processing sensitive data – that should be subject to consent. LD 1977 ignores this guidance, and would require consent for first-party advertising. This will be deleterious for businesses in the state that use first party advertising to reach consumers more efficiently and at lower cost than, for instance, newspapers.

Consumers benefit from this approach because it ensures they do not get overwhelmed with consent requirements. We believe that the opt-in requirements regarding the transfers of covered data dilutes the protections and effectiveness of the opt-in mechanism for sensitive data because it creates unnecessary obstacles for consumers.

LD 1977 creates an overly expansive scope of the term "sensitive data" as compared to other state laws and FTC guidance. When combined with the broad opt-in requirements, this will be disruptive to the consumer experience. This is because it threatens to obscure the use of opt-in consent for the truly sensitive uses of data regarding reproductive care and gender-affirming care. If consumers get used to clicking through opt-in mechanisms routinely, the mechanisms will cease to be a signal that there is truly sensitive information being collected or shared. This is known as "consent fatigue," and occurs around, for example, the GDPR cookie banners that consumers regularly click through just to access the services and information they seek.

Additionally, this legislation prohibits businesses from collecting or processing sensitive data, except in limited circumstances where the collection and processing is deemed "strictly necessary." This standard requires businesses to make educated guesses about the collection and processing of consumer data. Businesses that, in good faith, attempt to comply with this legislation may still find themselves in non-compliance.

LD 1977 Threatens to Repeat California's Mistakes

While the template largely followed by LD 1973 has been adopted in 11 states and has significant momentum in other New England states as well, the California Consumer Privacy Act (CCPA) has not been passed in a single other jurisdiction due to its many flaws. If LD 1977 were to pass, Maine would risk replicating these mistakes.

There are several reasons for this. First, it is extremely difficult to understand and comply with, and is correspondingly expensive to implement. California estimated that its initial compliance costs would be at least \$50,000 per company. Because much of LD 1977 is not interoperable with other states, the compliance costs on businesses is likely to be similarly exorbitant.

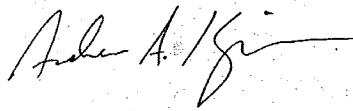
Second, the CCPA is far too prescriptive and granular, and in so doing is extremely difficult to adapt to new technologies and concepts. Similarly, LD 1977 is extremely granular; as a result, it would be difficult to continually add new concepts to the legislation as new technologies and issues emerge. In contrast, Connecticut last year was able to modify its legislation to include consumer health data, which was possible because there was a framework in place to do so without fundamentally adding new terms or concepts.

STATE PRIVACY & SECURITY COALITION

Lastly, it does not use similar terms and works differently than the other 11 states. In addition to the disproportionate compliance cost described above, this independently hinders interoperability with other states' privacy laws creating burdens for businesses and consumers alike.

We thank you in advance for your continued work and consideration. We look forward to the opportunity to discuss these important issues in person.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Andrew A. Kingman". The signature is fluid and cursive, with a long horizontal stroke at the end.

Andrew A. Kingman
General Counsel, State Privacy & Security Coalition