That's a Baker's Dozen: New Jersey Becomes 13th State to Pass Comprehensive Consumer Data Privacy Legislation

January 12, 2024

By: Alfred Brunetti

In a bit of an early year surprise, New Jersey became the 13th[1] state to pass a comprehensive-style consumer data privacy law. Passage came on Monday, January 8, just hours before the State's legislative session expired. In a somewhat dramatic fashion, Senate Bill 332 (Bill) underwent significant revisions and amendments in the closing days of 2023 to morph from a narrow, operator-centric draft into a more comprehensive bill with notable obligations and rights more closely aligned to the statutory privacy schemes in California, Colorado, and Virginia.

Assuming the signature by Governor Murphy in the coming days, the Bill would go into effect in 2025. Here's what you need to know now about what may soon become the New Jersey Consumer Data Privacy Act.

Who Will It Apply To?

If you are an individual or entity that conducts business in New Jersey or produces products or services targeted to New Jersey residents, the Bill will apply to you if, within a calendar year, you either: (a) control or process the personal data, other than for certain payment transaction processing, of at least 100,000 New Jersey residents (who are acting in an individual or household context); or (b) control or process the personal data of at least 25,000 New Jersey residents (who are acting in an individual or household context) and you derive revenue or receive a discount from the sale of personal data.

The Bill will apply equally to for profit, non profit and not for profit entities. Given New Jersey's population, this 100,000 resident threshold means that if you control or process the personal data of less than just 2% of the State's residents, you are within the scope of the Bill. And, once you are within its scope, the Bill will impose certain obligations upon you and afford certain rights to those individuals whose personal data you collect.

What Should I Be Thinking About Now?

If the Bill will apply to you, here are some considerations to keep in mind when evaluating your business practices:

1. Be certain you fully understand how you (or anyone else on your behalf) collect data, what data you collect, and what you do with that data. The Bill, like numerous other states' privacy laws, will require you to publish a consumer-facing privacy statement that sets forth various specified representations. Those representations will need to be accurate at all times so its creation and publishing is not a set-it-and-forget-it activity. Keeping atop your data practices is an ongoing obligation.

2. Obtaining specific, informed, and unambiguous consent will be a prerequisite to collecting or using certain types personal data but the collection of any personal data will be limited to what is "adequate, relevant and reasonably necessary" in relation to the purpose for which it is being collected. A firm grasp on the type of user experience and user interface your consumer-facing website deploys will be central to this task because using manipulative designs (however broadly that may be perceived by the Federal Trade Commission) will void any purported consent you may receive.

3. Appreciate the types and nature of data that you'll be collecting and intending to process. Various categories of data will be considered "sensitive data," and, as such, will need to be treated with special care. Some standards have begun to develop across the active state privacy schemes in this regard but under the Bill, even mainstay sensitive data categories like "biometric data" are more expansively defined than in other states. Uniquely in California – and now in New Jersey – certain "financial information" will also need to be treated as "sensitive data."

4. Make sure that operationally you have the resources and tools to deliver on the consumer rights you will be obligated to provide. That means not only ensuring good customer management practices and data inventory hygiene but also fostering end-to-end stewardship over your contractual relationships with vendors and third parties because your obligations as a "controller" of data cannot be delegated away and will need to be expressly set forth in data processing addenda.

5. Don't Panic. The Bill will not come into effect until one year after it is signed by Governor Murphy. It is almost certain that during that period, the Division of Consumer Affairs will promulgate rules and regulations which would clarify some of the more nuanced and novel aspects of the current law like, for example, its requirement that Universal Opt Out Mechanisms (UOOMs) be recognized to support users opting out of profiling and the contours of what qualifies as a "heightened risk of harm," a categorization that will trigger the creation of a Data Protection Assessment. Any specific rules or regulations may serve to bring the Bill's implementation into clearer focus as its anticipated effective date approaches.

At Porzio, we always welcome the opportunity to discuss the ever-changing business landscape with clients and friends to ensure that both their practices and compliance procedures are optimized. As we face the New Year, and the patchwork of state-specific consumer and health data privacy laws continue to expand and mesh with the increasingly frequent enforcement activities of the Federal Trade Commission and other important regulators, there's no better time to check in and have those discussions.

---

[1]Although Florida has also passed its Digital Bill of Rights, because that law will only apply to the relatively small universe of data controllers with an annual global revenue of more than $1 Billion, it is not typically grouped together with the collection of other states with consumer data privacy laws.