Thinking Precisely About Data Privacy in Florida

As more parts of our lives have moved online, so too have our data. These bits of personal information are key to the applications and services that we use every day. They are also valuable and sensitive, and it's important to think carefully about how our data are being used and safeguarded.

The Florida legislature has taken up the cause of data privacy in its 2021 session. Some parts of the proposals provide steps to updating our data rules which have been mostly concerned with notifying affected users in the wake of a data breach. Others may make it more costly to comply with regulations in the state of Florida without meaningfully improving privacy. Most concerningly, a new private right of action for violations of new data rules could merely provide a new avenue for trial attorneys to enrich themselves without much benefit to affected users.

Protecting Floridian's privacy online is a laudable goal. Here are a few tradeoffs that policymakers should consider as they look to update the state's data regulations.

The proposals on the table

There are two bills, HB 969 and SB 1734, that aim to address data privacy working their way through the Florida legislature. The measures would apply to companies that specialize in data operations (either buying, selling, or receiving the data of 50,000 people or earning at least 50 percent of global annual revenue from selling or sharing data)—the House version also includes large businesses with gross annual revenues in excess of $25 million.

The proposals outline a number of new obligations and penalties surrounding online data. Covered entities must maintain a regularly updated privacy policy, inform users how they will store and use personal data, allow users to request, correct, or delete data, and allow users to opt out of the sharing of their personal data. The bills also enhance existing enforcement around data breach laws, most notably in the House version by creating a private right of action for Floridians to sue businesses that violate established law.

More time is better

From the start, legislators should consider that a sweeping change in data privacy rules necessitates sweeping process changes in the private businesses that will comply with the new rules. Currently, the House bill is set to take effect on January 1, 2022 (the Senate version would take effect on July 1, 2022). This would leave businesses with around a year to get their systems updated to comply with the expanded rules. To give businesses and the new law the greatest chances for success, legislators could consider easing the enactment date until 2023 or later.

Think carefully about private rights of action

Florida's previous data breach notification law was enforced by Florida's Department of Legal Affairs (FDLA). The House version of the bill would create a private right of action for data breach damages ranging from $100 to $750 per user per incident. Given that data breaches can affect millions of users, these costs can quickly add up. Proposed amendments have gone farther to include the right to recoup lawyer's fees from these lawsuits, which is reminiscent of Florida's personal injury protection (PIP) law which has led to inflated legal and insurance costs in Florida.

It is important that the state's enforcement mechanism is commensurate to facilitate the law without creating new costs that do not meaningfully improve Floridians' privacy. Legislators could consider strengthening the state's current administrative enforcement through FDLA (indeed, other portions of the proposals do just that) rather than introducing a potentially expensive and counterproductive private cause of action.

The JAMES MADISON INSTITUTE
Trusted Solutions for a Better Florida

Keep definitions tight and in line with national and international standards

In the absence of a federal data privacy law, other states have stepped in with their own laws. California, Virginia, and Washington are just a few of the states that have passed or are considering state data privacy laws. While these states all take their own unique approaches, and these have their own benefits and downsides, it is important that Florida's law stay consistent with the broad definitions common to these laws. If not, Florida's law risks being a higher compliance risk, and therefore could make our state less attractive for business and growth.

Specifically, legislators should take care that definitions of regulated terms are tight and in line with developing national standards.

Don't lock in specific technologies that might soon be obsolete

In general, policymakers should avoid locking in today's technological arrangements through regulations that may one day prove outdated. Businesses should not be stuck to outdated processes because of compliance risks. Therefore, legislators should take care that data privacy rules allow room for experimentation and innovation in terms of data management and privacy arrangements.

Putting it all together

Data privacy policy is a complex subject in a fast-moving digital world. The Florida legislature is considering proposals that build on the state's data breach notification framework to include new obligations for data policy transparency and user rights. This is laudable. By considering best practices from other states and weighing the trade-offs between different enforcement mechanisms and deadlines, policymakers can serve both Floridians' privacy interests as well as our pro-enterprise climate that has made the state so attractive to so many new residents and firms.

For any questions on JMI's principles on data privacy, please contact Andrea O'Sullivan at Andrea@JamesMadison.org