BUSINESS LAW SECTION OF THE FLORIDA BAR
COMPUTER AND TECHNOLOGY LAW COMMITTEE

WHITE PAPER IN SUPPORT OF PROPOSED POLICY ON DATA SECURITY AND PRIVACY

SEPTEMBER 2, 2020

I. BACKGROUND

In the last two consecutive legislative sessions (2019 and 2020), data privacy and cybersecurity bills have been introduced in Florida. With over forty bills being introduced nationwide between 2018 and 2020, and three states (California, Maine, and Nevada) already having enacted comprehensive data privacy laws, the forecast is for Florida to see at least one data privacy or cybersecurity bill introduced in each of the next several years.

In addition, three other states (Illinois, Texas, and Washington) have enacted biometric data privacy laws that focus on a particular subset of information relating to the commercial collection and use of an individual's physical attributes (e.g. fingerprints, facial recognition, retina scans, etc.). A bill introduced in Florida in 2019 focused on this particular subset of data, highlighting Florida legislators' interest in addressing these novel issues in this state. While Illinois' statute provides for a private right of action, Texas' and Washington's statues provide for enforcement by their state attorneys general. A number of other states, including Alaska, Arizona, Connecticut, Delaware, Massachusetts, Michigan, New Hampshire, and New York similarly entertained bills potentially regulating the collection and use of biometric data in recent years.

The anticipated impact any proposed legislation would have on Florida's businesses continues to evolve as different regulatory regimes are devised and passed across the nation. Given the high likelihood that Florida – among many of its sister states – may see more comprehensive and/or specialized data privacy and cybersecurity bills introduced for debate in the legislature in the near future, this Committee believes it to be prudent and wise to adopt a policy regarding such proposed legislation.

II. PROPOSED POLICY POSITION

Specifically, the Committee seeks for the adoption of the following legislative policy position, as approved by Motion at its regular meeting on September 2, 2020, providing that the Committee:

> **Supports legislation relating to data privacy and protection, including cybersecurity, that strikes the appropriate balance between protecting personal information without placing undue restrictions on business development or unnecessarily stifling technological advancement in this State.**

III. COMMENTARY ON PROPOSED POLICY

Adoption of this policy position recognizes the near inevitability of legislation on this issue. The policy position seeks to ensure that any such legislation provides a reasonable level of protection of personal information, while permitting the continued growth of business interests in Florida. This is especially important in light of the value businesses gain and the enhanced services

users receive from the business's use of the data, including improvements to cybersecurity. By adopting the proposed legislative policy, the Committee can more precisely focus its attention and resources on swiftly responding to, and providing substantive input on, proposed data privacy and cybersecurity bills that will likely be proposed in the near future.

In particular, a study of the two most recent proposals filed with the legislature demonstrates both the likelihood of additional legislative proposals on this subject in the near term and the need for well-articulated input to enable legislators to make an informed evaluation of such proposals going forward.

Notably, only a few Florida laws regulate the protection of personal information and data. Specifically, the Florida Information Protection Act, section 501.171, Fla. Stat., generally requires businesses in the state to provide for appropriate data security, to establish disposal requirements (i.e., retention rules), and to provide notices in the event of qualifying data breaches. Another privacy-related law includes section 1002.222, Fla. Stat., which prohibits public schools and agencies from collecting biometric information of a student, parent, or student's sibling. It is anticipated that Florida will follow the general trend toward more comprehensive and/or specialized data privacy regulation, or to amend its existing breach notification law to reflect industry norms as other states are doing with increasing frequency.

A. 2019 Florida Biometric Information Privacy Act

In 2019, the "Florida Biometric Information Privacy Act," was introduced as House Bill 1153 and Senate Bill 1270. The Act proposed to regulate the collection and use of biometric information. Biometric information, as defined by the bill, would consist of any information that can be used to identify a person based on biometric identifiers, such as retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry.

HB 1153 was drafted to provide that an organization may not "collect, capture, purchase, receive through trade, or otherwise obtain" biometric identifiers or information (collectively, biometric data) unless:

> (i) it provides written notice stating that
>
> > biometric data is being collected or stored, and
> >
> > the specific purpose and length of term for which biometric data is being collected, stored, and used; and
>
> (ii) it receives a written consent that is executed by either the individual whose biometric data is to be collected or the individual's legally authorized representative."

Further, HB 1153 proposed creating a private right of action for "any person aggrieved" by a violation of the statute and would have provided for statutory damages of $1,000 for a negligent violation to $5,000 for an intentional or reckless violation, in addition to reasonable attorneys' fees and costs.

This Committee previously expressed concern with the regime proposed by HB 1153. The private right of action proposed by that bill was modeled on the Illinois' Biometric Information Privacy Act., 740 Ill. Comp. Stat. 14/1-99. Already, we observed some companies altering their behavior in Illinois to adhere to the law. For example, Nest, a maker of smart thermostats and doorbells, sells a doorbell with a camera that can recognize visitors by their faces. In response to the Act, however, Nest refused to offer that feature in Illinois. (Source). In addition, we noted then, as we do now, that retailers, banks, and consumer product manufacturers are increasingly relying on biometric-based identification technology to allow consumers to authenticate purchases, to help direct consumers to specific products in physical stores, and to prevent shoplifting and other crimes. A restrictive biometrics statute could chill these technological benefits for Florida consumers and businesses.

Further compounding this issue, in January 2019, the Illinois Supreme Court ruled in *Rosenbach v. Six Flags*, 2019 IL 123186, that a plaintiff suing under BIPA need not allege or show actual injury or an adverse effect to maintain an action for damages. It was anticipated that this decision would result in an increase in class action lawsuits, and that prediction proved accurate. (Source). Therefore, we cautioned that it was anticipated that Florida businesses, consumers, and employers would experience the same potentially adverse effects as Illinois if HB 1153 were to pass (it did not).

The Committee is of the opinion that adoption of the reasonable policy articulated above would further the collective interest of advocating for legislation seeking to mitigate such issues, so as to provide adequate protections for individuals while not stifling development in this state.

B. 2020 Consumer Data Privacy Bill

In 2020, companion bills introduced in the legislature as Senate Bill 1670 and House Bill 963 were a clone of the Nevada's Consumer Privacy Law. They proposed to prohibit the use of personal data contained in public records under certain conditions, to require certain businesses to maintain an online privacy policy with certain information about their personal information collection and use, to prohibit such businesses from "selling" consumer information to third parties, and to require those businesses to honor opt-out requests received by Florida consumers upon request. The bill presented several potential problems. Among them were potential issues for implementation given its limited scope (governing the collection of personal data through a website or over the internet), which may not be easily segregated when businesses use parallel collection channels, and ambiguities in drafting that could open the bill up to constitutional challenges. Further, the bill left uncertain how businesses were to "verify" requests from consumers, and it provided no mechanism for state regulators to develop standards for implementation by businesses in verifying requests from consumers. In addition, the bill lacked cohesion with respect to the notice of rights afforded by consumers, providing for the identification of certain rights while wholly omitting notification as to others, which could mislead consumers or leave them unaware of their rights.

IV. CONCLUSION

Given the concerns with the two proposed bills introduced in Florida in the past two years, the frequency with which data privacy bills have been introduced across the nation (and internationally), and the likelihood that this trend will continue in Florida and throughout the country, this Committee proposes to adopt the reasonable policy articulated above to enable it to provide guided, effective, rapid, and substantive commentary and suggestions in response to any bills that may arise in the future.