The Florida Justice Reform Institute Opposes CS/CS/HB 969

2021 CS/CS/HB 969 proposes comprehensive consumer data privacy protections, including the creation of new obligations for covered businesses and the significant expansion of consumers' rights concerning businesses' use of personal information. While the bill is well-intentioned, the Florida Justice Reform Institute opposes the legislation as it would impose exceedingly burdensome and costly requirements on businesses with little benefit to consumers and create a broad private cause of action that will prove to be a boon for class action plaintiffs' lawyers.

The Compliance Requirements Are Onerous, Costly, and Needlessly Complex. The legislation's ostensible goal is to better protect consumers' personal information in the hands of businesses. CS/CS/HB 969 defines the term "personal information" to mean traditionally sensitive, personally identifying information like social security numbers and medical information—the types of information the disclosure of which risks identity theft. But the definition of "personal information" also encompasses relatively innocuous information, the disclosure of which is unlikely to lead to identify theft, such as "[i]nferences drawn from any of the [other types of personal information identified] to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." Proposed § 501.173(1)(m)1.k., Fla. Stat. Thus, for example, the inference that a consumer likes true crime shows based on his or her Netflix preferences is protectable "personal information" within the meaning of the legislation.

Under CS/CS/HB 969, covered businesses would be required to meet numerous requirements in order to protect such personal information, including the following: maintain an online privacy policy with detailed information regarding, among other things, the categories of personal information the business collects or has collected about consumers and which of those categories the business sells or shares or otherwise discloses to third parties (proposed § 501.173(2)(a), Fla. Stat.); implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information to protect the information from unauthorized or illegal access, destruction, use, modification, or disclosure (proposed § 501.173(2)(e), Fla. Stat.); and provide and follow a retention schedule that prohibits the use and retention of personal information after satisfaction of the initial purpose for collecting or obtaining such information, or after the duration of a relevant contract, or one year after the consumer's last interaction with the business, whichever occurs first (proposed § 501.173(2)(g), Fla. Stat.).

A covered business will be required to promptly respond to a consumer's request to copy, delete, or correct personal information, absent an applicable exemption. *See* Proposed § 501.173(3), (4), (5), Fla. Stat. Specifically, a business must act on such a request "free of charge within 45 days" after receiving the request, although the period may be extended "once by 30

additional days when reasonably necessary," taking into account the complexity of the consumer's request. Proposed § 501.173(8)(b), Fla. Stat.

These requirements are deceptively simple, but when applied to businesses' data management systems and practices, they are exceedingly complex and costly. Even for businesses with strong data management practices, the ability to identify and organize information, and make that information accessible and ready portable for consumers, would require a significant investment in additional data management software and program capabilities that can easily run into the millions of dollars. Indeed, most covered businesses do not inventory personal information to be sortable or retrievable by individual such that the requirements of the legislation can be accomplished easily. Given the breadth of the bill's definition of "personal information," companies will be required to translate the categories of information encompassed within that definition into discrete data elements so that they can catalogue and make accessible such information, all at great cost to the organization. Even when the legwork of readying systems to respond to consumer requests is done, the reality is that it will be difficult for a covered business to respond to all such requests within even the extended 75-day timeframe.

The legislation contains detailed exemptions for certain types of information, including, e.g., "personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act" ("GLBA"), a federal law that already requires financial institutions to explain information-sharing practices to their consumers and to safeguard sensitive personal data. Proposed § 501.173(10)(b)10., Fla. Stat. Such exemptions create their own complexities, as to account for these exemptions, covered businesses will have to invest significant amounts of resources into data management software and solutions that would allow them to appropriately catalogue personal information that is subject to CS/CS/HB 969 and that which is not (but may be subject to other, different requirements such as GLBA).

The legislation's requirement that covered businesses delete personal information upon request also presents unique challenges. In some instances, data meeting the legislation's definition of "personal information" might serve as a "key" between upstream and downstream systems, such that the attempted deletion of that "key" information will have consequences for the systems' overall stability and require covered businesses to conduct extensive testing before any data can be deleted—all the while running on a difficult-to-meet 45-day or 75-day clock.

In short, the legislation would require covered businesses to invest significant time and resources in compliance with Byzantine data management requirements to protect information as simple as a consumer's Netflix preferences. And that compliance will come at a great cost. As just an example, under the California Consumer Privacy Act ("CCPA") on which CS/CS/HB 969 appears to be modeled, the total estimated cost of ***initial*** compliance by businesses with the act was ***approximately $55 billion***.[1] This is ***in addition*** to the significant costs businesses will face as the result of the expansive civil liability proposed under CS/CS/HB 969, discussed next.

CS/CS/HB 969's Private Cause of Action Will Create a Gold Rush for Class Action Plaintiffs' Attorneys. There is no statutory private cause of action as of yet in Florida for data

[1] California Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act Regulations* at 11 (Aug. 2019), https://www.tellusventure.com/downloads/privacy/calif_doj_regulatory_impact_assessment_ccpa_14aug2019.pdf.

210 S. Monroe St. ● Tallahassee, FL 32301-1824 ● 850.222.0170 ● FAX: 850.222.1098

breaches. Under proposed section 501.173(12), Florida Statutes, a consumer would have a private cause of action where a covered business fails to:

- protect certain personal information which may be used to access an account and such information "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and practices";

- delete or correct a consumer's personal information pursuant to the consumer's request; and/or

- refrain from selling or sharing a consumer's personal information after the consumer opts out under the proposed law.

A consumer stating such a cause of action would be able to recover statutory damages of at least $100 and not more than $750 per consumer per incident or actual damages, whichever is greater, as well as attorneys' fees if the consumer prevails. Notably, the legislation does not contain an express causation requirement. Until now, the biggest obstacle plaintiffs faced in data breach litigation was proving actual harm—e.g., money losses. CS/CS/HB 969 removes that hurdle, and with the broad liability created under the proposed legislation, Florida will be the site of a new gold rush for class action plaintiffs' attorneys looking for easy and lucrative cases.

If CS/CS/HB 969 is passed, Florida will be aligning itself with California, which in 2018 passed the CCPA. The CCPA grants a similar private cause of action to consumers for data breaches. Specifically, under the CCPA, consumers may bring a civil action if their "nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Cal. Civ. Code § 1798.150(a)(1).[2]

Although the CCPA's private cause of action is ostensibly narrow, civil litigants have already begun pushing the boundaries of this provision. Indeed, law firm Akin Gump reports that "of the 76 consumer class actions filed in 2020 that allege some violation of the CCPA, at least 44—***more than half of all cases***—do not specifically allege that the plaintiff's personal information was subject to unauthorized theft or disclosure resulting from a business's violation of its duty to implement and maintain reasonable security procedures and practices."[3] In other words, the plaintiffs in most CCPA actions do not allege that personal information was actually subject to any data breach. Rather, most of these cases illustrate that opportunistic plaintiffs are alleging technical violations of the CCPA to support causes of action outside the CCPA, such as violations of other consumer protection statutes like California's Unfair Competition Law. Here are just three examples of class actions in which plaintiffs have invoked the CCPA notwithstanding the fact that no personal information was subject to a data breach:

---

[2] As discussed later, the CCPA does not provide the two other bases for a private cause of action that are included in CS/CS/HB 969.

[3] Akin Gump, *2020 CCPA Litigation Report: Trends and Developments* at 7 (available by request via https://sites-akingump.vuturevx.com/16/3798/landing-pages/2020-ccpa-litigation-report--trends-and-developments.asp).

210 S. MONROE ST. ● TALLAHASSEE, FL 32301-1824 ● 850.222.0170 ● FAX: 850.222.1098

- *In re: Zoom Video Communications, Inc. Privacy Litigation*, Case No. 5:20-cv-2155-LHK (N.D. Cal. 2020). Fourteen class actions against Zoom were consolidated in the Northern District of California, including one class action led by a class representative from Florida. These plaintiffs generally alleged that Zoom had shared consumers' personal information with third parties without consent and failed to implement protocols to properly safeguard consumers' information, all in violation of the CCPA and other consumer protection laws. Each action alleged a matter in controversy exceeding $5 million. Plaintiffs did not, however, allege that any personal information was the subject of an unauthorized access and exfiltration, theft, or disclosure as a result of the business's failure to implement and maintain reasonable security measures—the trigger to state a private cause of action under the CCPA. Plaintiffs appear to have dropped their CCPA claims in a later consolidated amended complaint, however, likely due to their failure to state an actual CCPA claim and their failure to notify Zoom before bringing suit as required by the CCPA.

- *Hayden v. The Retail Equation, Inc.*, No. 8:20-cv-01203-DOC-DFM (C.D. Cal. 2020). In *Hayden*, plaintiffs seek to represent a class of consumers and complain that, without consumers' consent or knowledge, Sephora USA, Inc. ("Sephora") shared consumers' personal information with The Retail Equation, Inc., which in turn created consumer reports for Sephora. The complaint does not allege an express claim under the CCPA's private cause of action provision, and likely cannot, because the plaintiffs do not allege that any personal information was the subject of "an unauthorized access and exfiltration, theft, or disclosure as a result of the business's failure to implement and maintain reasonable security measures." Instead, plaintiffs attempt to state other causes of action—e.g., an unfair competition claim—based on violation of the CCPA's notice and disclosure provisions. Defendants have moved to dismiss on various grounds, including on the grounds that violation of the notice provisions of the CCPA does not give rise to a private cause of action and no personal information has been subject to a data breach. Defendants' motion to dismiss remains pending.

- *Conditi v. Instagram, LLC*, No. 3:20-cv-06534 (N.D. Cal. 2020). In this class action, plaintiffs allege that Instagram accesses consumers' smartphone cameras without consumers' consent. Plaintiffs allege that Instagram's conduct violates the CCPA because Instagram failed to disclose that it monitors users through their smartphone cameras "to collect personal information." Plaintiffs do not, however, state an actual cause of action under the CCPA, but simply argue that the CCPA violation of "monitoring" users amounts to, e.g., a claim under California's Unfair Competition Law. The case remains pending, and defendants have been given additional time to file a motion to dismiss.

These cases illustrate that, notwithstanding the express language of the CCPA, class action plaintiffs' attorneys can and will find ways to push the limits of any new private cause of action. Perhaps of greater concern here is the fact that CS/CS/HB 969 will likely prompt ***more*** litigation than the CCPA, for at least a few reasons:

- The private cause of action that would be authorized under CS/CS/HB 969 is ***broader*** than that in the CCPA. In addition to data breaches—i.e., where personal information is subject to "an unauthorized access and exfiltration, theft, or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and

210 S. MONROE ST. ● TALLAHASSEE, FL 32301-1824 ● 850.222.0170 ● FAX: 850.222.1098

practices"— CS/CS/HB 969 would grant additional private causes of action, including any time a business fails to, for example, ***delete every piece of personal information related to a consumer after receiving a consumer's deletion request***. *Compare* Cal. Civ. Code § 1798.150(a)(1), *with* Proposed § 501.173(12)(a)2., Fla. Stat.

- Under the CCPA, before bringing suit, a consumer must notify the business and identify the specific provisions of the CCPA that the business purportedly violated. Cal. Civ. Code § 1798.150(b). The business then has 30 days to cure the noticed violation, to the extent a cure is possible. *Id.* ("if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business"). Under CS/CS/HB 969, the only opportunity for notice and cure is afforded by the Department of Legal Affairs, and even then, a business's cure of the violation has absolutely no impact on the liability the business faces from consumers. Proposed § 501.173(13)(c), (d).

- Another striking difference is that although the CCPA's definition of the term "personal information" is broad, a much narrower definition of that term applies to the private cause of action. *See* Cal. Civ. Code § 1798.150(a)(1); Cal. Civ. Code § 1798.81.5(d)(1)(A) (defining "personal information" for purposes of the private cause of action to mean more traditional personally identifying information, such as, e.g., a social security number, account number, driver's license number, and medical information). In contrast, CS/CS/HB 969 incorporates its broad "personal information" definition—to include even internet browsing history and consumer preferences, data elements the disclosure of which pose virtually little risk of identity theft—into the private cause of action. Thus, the failure of a business to scrub from its files a note about a consumer's preference for true crime shows would potentially trigger a private cause of action under CS/CS/HB 969 and the opportunity for at least statutory damages.

Even aside from these concerns, the private cause of action proposed by CS/CS/HB 969 will likely devolve into expensive litigation that will almost always require jury trials. For example, the question whether a business complied with the duty to maintain and implement reasonable security procedures and practices will inevitably be a factual question that will require extensive discovery and litigating, and is unlikely to be resolved prior to a costly and lengthy trial. Thus, even if the plaintiff is ultimately unable to prove that the data breach was the result of the business's failure to implement and maintain appropriate security practices within the meaning of the law, the business will still have spent hundreds of thousands of dollars defending the lawsuit in the meantime.

The Proposed Cause of Action Is Inconsistent with Florida's Data Breach Notification Law. The definition of what constitutes a data breach, triggering the private cause of action proposed in CS/CS/HB 969, is also inconsistent with the definition of a data breach under Florida's data breach notification law, which may have significant negative consequences for consumers.

Florida's data breach notification law requires businesses to implement reasonable data security measures and requires covered businesses experiencing a data breach within the meaning of the law to notify consumers and the Department of Legal Affairs. *See* § 501.171, Florida

210 S. MONROE ST. ● TALLAHASSEE, FL 32301-1824 ● 850.222.0170 ● FAX: 850.222.1098

Statutes. Under CS/CS/HB 969's private cause of action, "an unauthorized access and exfiltration, theft, or disclosure" of certain personal information is a data breach authorizing a consumer to bring suit. In contrast, Florida's breach notification law limits the definition of a breach to "unauthorized access of data in electronic form containing personal information." § 501.171(1)(a), Fla. Stat.

The differences in these definitions mean this: it is possible that under CS/CS/HB 969, a business might be sued based on a data breach for which it would not have been required to give notice under the data breach notification law. This may create a disincentive for businesses to notify the Department of Legal Affairs and consumers that a breach has occurred because bringing attention to the issue means the business would be risking significant statutory liability under CS/CS/HB 969's private cause of action. Such a disincentive would in turn only make it more difficult for consumers to learn about and resolve data breaches involving their personal information.

Vote No on CS/CS/HB 969. CS/CS/HB 969 would create a complex and flawed data privacy law with little if any tangible benefits for consumers. Only class action plaintiffs' attorneys stand to benefit, as the act would present a lucrative opportunity to build class actions based on technical violations of the law, notwithstanding the fact that such violations did not lead to actual consumer harm. Florida already has sufficient laws to protect against data breaches, including the data breach notification law under which the Attorney General may seek up to $500,000 in civil penalties against businesses which violate the law. *See* § 501.171(9), Fla. Stat. For all these reasons, the Florida Justice Reform Institute urges that you vote no on CS/CS/HB 969.

210 S. Monroe St. ● Tallahassee, FL 32301-1824 ● 850.222.0170 ● FAX: 850.222.1098