April 28, 2023

Speaker Paul Renner
Majority Leader Michael Grant
Minority Leader Fentrice Driskel
Florida House of Representatives
402 South Monroe Street
Tallahassee, FL 32399

Re: Florida H.B. 1547, Consumer Privacy Legislation— OPPOSE

Dear Speaker Renner, Majority Leader Grant, and Minority Leader Driskel,

Consumer Reports[1] writes in respectful opposition to H.B. 1547, consumer privacy legislation. The bill seeks to provide to Florida consumers the right to know the information companies have collected about them, the right to access, correct, and delete that information, as well as the right to stop the disclosure of certain information to third parties. However, due to its applicability to only the very largest tech companies and other significant loopholes, it would leave Florida consumers' personal information unprotected in a wide variety of contexts. As such, the bill's scope should be substantially widened before it is enacted.

Consumers currently possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they collect and process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers' every move is constantly tracked and often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

At the same time, spending time online has become integral to modern life, with many individuals required to sign-up for accounts with tech companies because of school, work, or simply out of a desire to connect with distant family and friends. Consumers are offered the illusory "choice" to consent to company data processing activities, but in reality this is an all or nothing decision; if you do not approve of any one of a company's practices, you can either forgo the service altogether or acquiesce completely.

As such, privacy laws should set strong limits on the data that companies can collect and share so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out. We recommend including a strong data minimization requirement that limits data collection and sharing to what is reasonably necessary to provide the service requested by the consumer, as outlined in our model bill.[2] A strong default prohibition on data sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially thousands of different companies.

However, even though H.B. 1547 is based on an opt-out regime, we note that it currently includes certain protections that should remain in place even as future amendments are considered:

- *Opt-outs apply to both data sales and sharing.* H.B. 1547's opt-out provisions apply broadly and manage to avoid a loophole present in many other privacy measures. For example, in California, many companies sought to avoid the CCPA's opt out requirements by claiming that many online data transfers are not technically "sales", but rather "shares" (CPRA subsequently expanded the scope of California's opt-out to include all data sharing and clarified that targeted ads are clearly covered by this opt-out). This bill's opt-out appropriately includes sharing, which is defined to include the type of commercial transactions that allow companies to leverage consumers' personal information for the purpose of targeted advertising.

- *Sectoral exemptions are conditional.* While H.B. 1547 does exempt all financial institutions and affiliates of a financial institution, as defined in the Gramm-Leach-Bliley Act, as well as covered entities and business associates under the Health Insurance Portability and Accountability Act, it makes those exemptions conditional. The exemptions only apply to the extent that businesses treat *all* personal information they collect as covered information under their operative sectoral privacy law and only if the

[2] *Model State Privacy Act*, Consumer Reports (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.

business does not use personal information for targeted advertising or sales. While Consumer Reports would prefer to see privacy legislation only exempt the *data* that is already covered by other sectoral privacy laws, this is an improvement over exempting institutions wholesale.

- *No authentication requirements for opt-outs.* While authentication requirements may be appropriate when consumers are requesting to access, delete, or correct their information, controllers should not be allowed to authenticate requests to opt-out. Fraudulent access, deletion, or correction requests can pose real consumer harm, such as identity theft or stalking. However, opt-out rights do not carry similar risks to consumers and therefore should not be subjected to this heightened standard. In the past, businesses have used authentication clauses to stymie rights requests by insisting on receiving onerous documentation. For example, in Consumer Reports's investigation into the usability of new privacy rights in California, we found examples of companies requiring consumers to fax in copies of their drivers' license in order to verify residency and applicability of CCPA rights.[3]

- *Prohibition on controllers hounding consumers for consent to override an opt-out*. Section 7(a)(2) clearly states that controllers must respect the consumer's decision to opt out for at least 12 months before requesting that the consumer opt back in. Many other privacy measures are silent on this point, which could allow controllers to respond to opt-outs with incessant requests to override. This both contravenes the spirit of increasing consumer autonomy expressed in these types of comprehensive privacy laws and could result in a frustrating and unwieldy consumer experience.

At the same time, the bill needs to be significantly strengthened in order to offer the protections that Flordians deserve. We make the following recommendations:

- *Require companies to honor browser privacy signals as opt outs.* Consumers need tools to ensure that they can better exercise their rights in an opt out regime, such as a global opt out option. While the bill currently gestures toward universal opt out by providing that controllers "may" honor universal opt out requests, it does not require it. By contrast, the California Privacy Rights Act, the Colorado Privacy Act, Connecticut Data Privacy Act, and recently passed Montana Consumer Data Privacy Act all require controllers to

[3] Maureen Mahoney, Many Companies Are Not Taking the California Consumer Privacy Act Seriously, Medium (January 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.

honor such requests.[4] Proposals in a number of states this year, including Kentucky (S.B. 5), Oklahoma (H.B. 1030), New Hampshire (S.B. 255), Rhode Island (H.B. 5745), Oregon (S.B. 619), New York (S.B. 365), and others include a similar provision.

Privacy researchers, advocates, and publishers have already created a "do not sell" specification designed to work with such frameworks, the Global Privacy Control (GPC).[5] This could help make the opt-out model more workable for consumers,[6] but unless companies are required to comply, it is unlikely that consumers will benefit. We recommend using the following language:

> *Consumers or a consumer's authorized agent may exercise the rights set forth in Section 2(4-6) of this act by submitting a request, at any time, to a business specifying which rights the individual wishes to exercise. Consumers may exercise their right under Section 2(6) via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt out.*

Notably, the "authorized agent" provision mentioned above would allow a consumer to designate a third party to perform requests on their behalf — allowing for a practical option for consumers to exercise their privacy rights in an opt-out framework. Consumer Reports has already begun to experiment with submitting opt-out requests on consumers' behalf, with their permission, through authorized agent provisions.[7] Authorized agent services are an important supplement to platform-level global opt outs. For example, an authorized agent could process offline opt-outs that are beyond the reach of a browser signal. An authorized agent could also perform access and deletion requests on behalf of consumers, for which there is not an analogous tool similar to the GPC.

- *Widen the applicability threshold.* H.B. 1547 only currently applies to entities that make over $1 billion in gross revenues per year and satisfy certain other conditions. As a result, this bill would only apply to the very largest tech companies. In the modern digital marketplace, size and revenue are poor proxies for an entity's capacity to collect and

---

[4] Cal. Code Regs tit. 11 § 999.315(c); CPRA adds this existing regulatory requirement to the statute, which went into effect on January 1, 2023, at Cal. Civ. Code § 1798.135(e) https://thecpra.org/#1798.135. For the Colorado law, see SB 21-190, 6-1-1306(1)(a)(IV)(B), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf. For the Connecticut law, see Public Act No. 22-15, Section 6(a)(A)(ii)
For the Montana law, see SB 384, Section 6(3)(b) https://leg.mt.gov/bills/2023/billpdf/SB0384.pdf

[5] Global Privacy Control, https://globalprivacycontrol.org .

[6] Press release, Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights, Global Privacy Control (Oct. 7, 2020), https://globalprivacycontrol.org/press-release/20201007.html.

[7] Ginny Fahs, Putting the CCPA into Practice: Piloting a CR Authorized Agent, Digital Lab at Consumer Reports (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8.

process large amounts of consumer data, and, by extension, create significant privacy risks. Cambridge Analytica, which illegally harvested the personal information of 87 million people, only employed 107 people at the time its unscrupulous practices were revealed in 2018 and made around $25 million in revenue the previous year.[8]

Florida would be the only state to include such a high threshold for coverage in an otherwise comprehensive privacy law. Even the weak Virginia Consumer Data Protection Act applies to smaller entities who nonetheless process consumer data as a core business practice. We urge the drafters to remove this provision and instead include coverage thresholds pegged to the amount of personal data a company processes.

- *Add a sensitive data opt-in provision*. Many companies that collect especially sensitive personal information are failing to safeguard it. For example, a 2021 Consumer Reports investigation into seven of the leading mental health apps showed that they had significant privacy issues: many sent user and device information to social media companies and all had confusing privacy policies that few consumers would understand.[9] Most consumers do not understand the bounds of existing privacy law. In a 2023 study headed by University of Pennsylvania researchers, 82% of consumers didn't realize that HIPAA does not apply to many health-related data in mobile apps.[10] Controllers should transparently communicate to consumers when they are collecting especially sensitive information, and this information should only be collected and processed if consumers give an affirmative opt-in consent.

- *Non-discrimination.* Consumers should not be retaliated against for exercising their privacy rights—otherwise, those rights are functionally meaningless. Unfortunately, Section 2(8)(b-c) of this bill could allow companies to deny service or charge consumers a different price if they exercise their rights under this bill. We urge you to adopt consensus language from the Washington Privacy Act that clarifies that consumers cannot be discriminated against for declining to sell their information, and limits the disclosure of information to third parties pursuant to loyalty programs:

> *A controller may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing*

[8] Peg Brickley, "Cambridge Analytica Revenue Fell as Questions About Data Tactics Surfaced," Wall Street Journal, (June 1, 2018) https://www.wsj.com/articles/cambridge-analytica-revenue-fell-as-questions-about-data-tactics-surfaced-1527883000; Pitch Book, Cambridge Analytica Overview, (May 2018), https://pitchbook.com/profiles/company/226886-68

[9] Thomas Germain, Mental Health Apps Aren't All As Private As You May Think, Consumer Reports, (March 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/

[10] Turow, J., Lelkes, Y., Draper, N. A., & Waldman, A. E. (2023). Americans Can't Consent To Companies' Use Of Their Data.

a different level of quality of goods and services to the consumer. This subsection does not prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program. If a consumer exercises their rights pursuant to Section 541.051(b)(5) of this act, a controller may not sell personal data to a third-party controller as part of such a program unless: (a) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.

- *Strengthen enforcement*. While we appreciate that the civil penalties authorized in the bill are substantial and that the "right to cure" provision is currently discretionary, we recommend removing the ability to cure altogether to ensure that companies are incentivized to follow the law.[11] In practice, the "right to cure" is little more than a "get-out-of-jail-free" card that allows businesses to avoid punishment when they are caught breaking the law. In addition, consumers should be able to hold companies accountable in some way for violating their rights—there should be some form of a private right of action.

We look forward to working with you to ensure that Florida consumers have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Policy Analyst

cc: The Honorable Jennifer Bradley
The Honorable Fionna McFarland

[11] At the very least, the right to cure should sunset like it does under the Connecticut Data Privacy Act. See Public Act No. 22-15, Section 11(b), https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF