NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 25, ISSUE 2: DECEMBER 2023

SURVEILLING BIG TECH: NAVIGATING CENSORSHIP CONCERNS AND CONSUMER PROTECTIONS IN FLORIDA'S DIGITAL BILL OF RIGHTS

Daniel C. Self*

In 2021, Florida passed Senate Bill 7072 in response to concerns of censorship from large Silicon Valley-based social media companies. After the Eleventh Circuit enjoined Bill 7072, Florida passed the Florida Digital Bill of Rights—a data privacy statute that also contained distinct anti-censorship provisions. After granting certiorari in Moody v. NetChoice, LLC., the U.S. Supreme Court should clarify how states may legislate anti-censorship provisions for social media companies. This Article provides two recommendations: (1) Florida should strengthen its consumer privacy protections by broadening the FDBR's applicability provisions; and (2) Florida should revise the FDBR's anti-censorship provision based on the holding in Moody.

TABLE OF CONTENTS

* J.D. Candidate, University of North Carolina School of Law, 2025. The Author would like to recognize the editorial staff of NC JOLT, with particular thanks to Brooke Siegal, Julia Rhys Vaughan-Jones, Hayfa Ayoubi, Sophia Vouvalis, and McGee Roman for their invaluable feedback and guidance throughout the publication process.

I. INTRODUCTION

In May 2023, the Federal Trade Commission and the U.S. Department of Justice ("DOJ") ordered Amazon to pay a $25 million civil penalty.[1] The cause? Despite filing deletion requests to Amazon, customers learned that the company had illegally retained their voices and geolocation data.[2] Rather than feigning ignorance, Amazon took the position that it actively knew its actions contravened federal privacy law.[3] Yet, the company justified its decision by claiming that these voice recordings helped improve their technology's response to voice commands.[4] In a particularly chilling line, the DOJ observed that people's "voice recordings provide Amazon with a valuable data bank for training the Alexa algorithm."[5]

---

[1] Press Release, Fed. Trade Comm'n, FTC & DOJ Charge Amazon with Violating Children's Privacy Law, (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever [https://perma.cc/8TGZ-9UE4].

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Complaint at 6, United States v. Amazon.com, Inc., 2:23-cv-00811-TL (W.D. Wash. Jul. 19, 2023).

When customers interacted with their Alexa device, Amazon saved their voice recordings both as an audio and text file, and marked those files with identifiers to link them to the customer's Amazon profile.[6] The company's privacy policy assured customers who owned an Alexa that they could delete their personal information at any time.[7] Yet, in practice, Amazon responded to deletion requests by only deleting the relevant voice recording while retaining the written transcript.[8] The company also designed Alexa's software to show that, when a user deleted a recording, "the 'play' button for the recording and the written text disappeared, suggesting that both the audio and text files had been deleted."[9] This design choice further supported the notion that if a person deleted their voice records, the recordings would be deleted *in totality*. Yet, contrary to this, the DOJ found that these "transcripts remained available for Amazon's benefit and use for product improvement—such as developing Alexa's voice recognition and natural language processing technology."[10]

The American news cycle seems inundated with stories of large technology companies collecting consumer data and then engaging in deceptive or illegal data collection and retention practices. In 2019, the Pew Research Center studied Americans' sentiment toward current data collection practices.[11] The Center found that over 60% of Americans believed that it was impossible to go through daily life without companies collecting their data.[12] Similarly, it found that over 80% of Americans feel little to no control over the data that companies collect.[13] Important to the political discourse, the study found that three out of four Americans

---

[6] *See id.*
[7] *See id.* at 7.
[8] *See id.* at 8.
[9] *See id.*
[10] *Id.*
[11] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 19, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/Y95W-48EJ].
[12] *Id.*
[13] *Id.*

are concerned with how companies use their personal data.[14] Likewise, a study conducted by Ipsos found that over 80% of Americans were concerned with the safety and privacy of their online data.[15] Another study found that over 70% of Americans support establishing national standards for how companies collect personal data and support treating data privacy for individuals as a national security threat.[16] Put simply, American citizens have become increasingly concerned with how the technology sector collects and retains their personal information, driving the topic to become a political issue of national importance.

In June 2018, California became the first state to implement comprehensive data privacy legislation by enacting the California Consumer Privacy Act ("CCPA").[17] In July 2023, Florida became the tenth state with the passage of their Digital Bill of Rights. The Florida Digital Bill of Rights ("FDBR"), which will take effect on July 1, 2024, aims to further protect consumer data—specifically, sensitive personal, political, and biometric information.[18] However, when compared with other states' data privacy laws, the FDBR's narrow applicability provision limits its effectiveness in protecting consumer data.

---

[14] *Id.*

[15] *See* Mallory Newall & Johnny Sawyer, *A Majority of Americans are Concerned About the Safety and Privacy of their Personal Data*, IPSOS (May 5, 2022), https://www.ipsos.com/en-us/news-polls/majority-americans-are-concerned-about-safety-and-privacy-their-personal-data [https://perma.cc/LDA5-K8RS]; *see also* ASSOCIATED PRESS-NORC CTR. FOR PUBLIC AFFS. RSCH., *Trust in Government is Low, But Americans Are United Around Investments in Technology* 2 (2021) ("More than 7 in 10 adults say the federal government should establish national standards for how companies collect, process, and share personal data to help protect the privacy and security of individuals in an increasingly online world.").

[16] *See id.*

[17] *Comply with US Privacy Laws*, DATAGUIDANCE, https://www.dataguidance.com/comparisons/usa-privacy-laws [https://perma.cc/R7JE-BMZ9] (last visited on Sept. 25, 2023).

[18] *See* F. Paul Pittman et al., *Florida Enacts the Digital Bill of Rights, Joining the Growing Privacy Landscape*, WHITE & CASE (Sept. 20, 2023), https://www.whitecase.com/insight-alert/florida-enacts-digital-bill-rights-joining-growing-privacy-landscape [https://perma.cc/MHG8-F3TS].

This Article recommends that the Florida Legislature amend the FDBR's applicability provisions to broaden the statute's scope. Part II recounts the legislative history preceding the FDBR and discusses the state's political motivations for passing the statute. Part III addresses the FDBR's narrow applicability provisions and outlines three alternative models. Part IV argues that while the FDBR serves an important role by implementing comprehensive data privacy legislation in Florida, limiting its focus to only large social media companies narrows its scope to the detriment of their constituents. Part V analyzes *Moody v. NetChoice, LLC* and outlines the anticipated arguments against Bill 7072's individualized-explanation provisions. Part VI recommends two amendments for the Florida to consider incorporating into the FDBR: (1) that Florida strengthen its consumer privacy protections by broadening the FDBR's applicability provisions; and (2) that Florida revisit the FDBR's anti-censorship provisions based on the verdict in *Moody*.

II. THE FLORIDA DIGITAL BILL OF RIGHTS: PASSAGE AND HISTORY

At first glance, the FDBR reads like most other recent state data privacy statutes, with provisions focused on the collection and retention of private consumer data.[19] However, a broader lens suggests that the FDBR is yet another installment in a long-standing, contentious legislative feud between the Florida Legislature and Silicon Valley-based social media companies. Florida Governor Ron DeSantis' statements made clear that the FDBR was drafted to target only large technology companies.[20] The FDBR's applicability provision—the section determining whether a company is subject to the Statute—contains language which makes the FDBR wholly inapplicable to smaller companies.[21]

---

[19] *Protecting Floridians' Digital Rights*, FLGOV.COM (June 2023), https://www.flgov.com/wp-content/uploads/2023/06/Digital-Bill-of-Rights59-scaled.jpg [https://perma.cc/BD5M-BH29].

[20] *See id.*

[21] FLA. REV. STAT. § 501.702(9)(a)(1) (2023).

The Florida Legislature often refers to "Big Tech" when outlining their censorship and data privacy concerns. However, identifying which companies the Legislature is referencing becomes a more significant challenge. Despite using this term in official press releases and publications, the Legislature does not outline what constitutes "Big Tech."[22] "Big Tech" is often used in reference to "a group of technology companies that have dominated the industry for years due to their size, influence, and financial success."[23] Colloquially, the term typically includes Amazon, Apple, Meta, Google, and Microsoft;[24] however, because of its loose definitions, "Big Tech" may also be read to include other large technology companies like Tesla, Nvidia, or Alibaba.[25]

A. Florida's Contentions with Big Tech

The Florida Legislature had set its sights on curtailing Big Tech years prior to the passage of the FDBR. Before passing the FDBR, Florida attempted to combat censorship from Big Tech via Bill 7072.[26] Bill 7072, often referred to as the "Stop Social Media Censorship Act," was enacted in the wake of former President Donald Trump's suspension from X ("Twitter").[27] In response, Bill 7072 aimed to "hold Big Tech accountable by driving transparency and safeguarding Floridians' ability to access and participate in online platforms."[28] In the wake of conservative political voices

---

[22] *See Protecting Floridians' Digital Rights*, *supra* note 19.

[23] *What Companies Fall Under Big Tech? How Do You Land a Job With Them?*, EMERITUS (Feb. 21, 2023), https://emeritus.org/blog/technology-big-tech/ [https://perma.cc/XD3E-FP3N].

[24] *See id*.

[25] *See* Alison Beard, *Can Big Tech Be Disrupted?*, HARV. BUS. REV. (Jan.-Feb. 2022), https://hbr.org/2022/01/can-big-tech-be-disrupted [https://perma.cc/WA44-KZYT].

[26] Fla. S. Comm. on Governmental Oversight and Accountability, 2021 Summary of Legis. Passed: SB 7072 – Social Media Platforms (2021).

[27] Amy Howe, *Justices Request Federal Government's Views on Texas and Florida Social-Media Laws*, SCOTUSBLOG (Jan. 23, 2023, 4:44 PM), https://www.scotusblog.com/2023/01/justices-request-federal-governments-views-on-texas-and-florida-social-media-laws/ [https://perma.cc/R46B-WERZ].

[28] Press Release, Gov't of Fla., Governor Ron DeSantis Signs Bill to Stop the Censorship of Floridians by Big Tech (May 24, 2021), https://www.flgov.com/2

being banned from a number of social media platforms, Bill 7072 was designed to prevent social media companies from banning and "de-platforming" politicians.[29] These provisions responded to a longstanding outcry from conservatives that social media companies "unfairly moderate[d] their speech."[30]

The Legislature's ongoing concerns of political censorship from "Silicon Valley elites" inspired Bill 7072.[31] DeSantis' statements upon the passage of Bill 7072 demonstrated the Florida Legislature's strong stance against Big Tech. As DeSantis claimed, "[m]any in our state have experienced censorship and other tyrannical behavior firsthand in Cuba and Venezuela. If Big Tech censors enforce rules inconsistently, to discriminate in favor of the dominant Silicon Valley ideology, they will now be held accountable."[32] Florida's Senate President Wilton Simpson, who raised concerns of "the abuses that are possible when [B]ig [T]ech goes unchecked,"[33] and House Speaker Chris Sprowls, who applauded Bill 7072 for standing up to "technological oligarchs and [for] hold[ing] them accountable,"[34] made analogous comments voicing their grievances with technology companies for censoring conversative viewpoints and speakers.

B. The History Behind Florida's Censorship Legislation

Both Bill 7072 and the FDBR include anti-censorship provisions addressing the concern of censorship and de-platforming of Republican politicians and voters. While conservatives have voiced complaints of censorship before, recent decisions from Google and

---

021/05/24/governor-ron-desantis-signs-bill-to-stop-the-censorship-of-floridians-by-big-tech/ [https://perma.cc/E3WS-ACLX].

[29] *See id; see also* Jon Brodkin, *Judges Block Florida Law That Says Facebook and Twitter Can't Ban Politicians*, ARSTECHNICA (May 23, 2022, 2:15 PM), https://arstechnica.com/tech-policy/2022/05/judges-block-florida-law-that-says-facebook-and-twitter-cant-ban-politicians/ [https://perma.cc/F4VZ-K2TR].

[30] Sara Morrison, *Florida's Social Media Free Speech Law Has Been Blocked*, VOX (May 24, 2022, 5:33 PM), https://www.vox.com/recode/2021/7/1/22558980/florida-social-media-law-injunction-desantis [https://perma.cc/A3FF-N5QT].

[31] Press Release, Gov't of Fla., *supra* note 28.

[32] *See* Morrison, *supra* note 30.

[33] *See id.*

[34] *See id.*

Twitter to ban well-known politicians from their platforms have exacerbated their frustrations.[35] Similarly, in the lead-up to the 2020 Presidential Election, Twitter's well-documented decision to block a potentially damaging story about Hunter Biden—the son of then presidential candidate Joe Biden—also served as a major catalyst in igniting a war between Big Tech and Republican politicians.

Tulsi Gabbard, a 2020 presidential candidate for the Democratic party, was the first notable politician to be de-platformed by a social media giant.[36] After participating in the presidential primaries in June 2019, Gabbard returned to find her Google campaign advertisement account suspended.[37] The reasoning for the suspension was not initially revealed, and all that Gabbard herself received was a notification from Google stating that the suspension had been implemented due to billing and advertising practice violations.[38] However, when Gabbard's team contacted Google, the company informed them that the suspension resulted from a terms of service violation.[39] While not explicitly stated, this event seemed to inspire Bill 7072's individualized explanation provisions, which required social media companies to provide notice when content is removed.

Many view Twitter's suspension of former President Donald Trump as the primary catalyst for the passage of Bill 7072. Following the January 6th insurrection on Capitol Hill, Twitter permanently banned Trump's account.[40] Twitter justified its decision based on its perception that the "risks of keeping his commentary on its site [were] too high."[41] However, Twitter noted that if Trump

---

[35] Lucia Rodriguez, *Freedom of Speech in the Era of Social Media*, 46 NOVA L. REV. 29, 41 (2021).

[36] *See* Carla Marinucci & Daniel Strauss, *Tulsi Gabbard Sues Google Over Post-Debate Ad Suspension*, POLITICO (July 25, 2019, 1:35 PM), http://www.politico.com/story/2019/07/25/tulsi-gabbard-sues-google-account-suspension-1435405 [https://perma.cc/JT6D-9DVY].

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] Kate Conger & Mike Isaac, *Twitter Permanently Bans Trump, Capping Online Revolt*, N.Y. TIMES (Jan. 12, 2021), http://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html [https://perma.cc/NGA9-BLGC].

[41] *Id.*

removed certain posts from his account, it would be reactivated.[42] The decision to ban Trump from Twitter received mixed responses. Supporters, such as Jonathan Greenblatt, CEO of the Anti-Defamation League, described Twitter's decision as "[a] fitting end to a legacy of spewing hate and vitriol,"[43] whereas critics argued that Twitter's decision to ban Trump was unprecedented and "deviat[ed] from the site's reactions to other heads of state who also incited or supported violence with their tweets."[44]

Republicans' censorship concerns also extend to the suppression of media that would be harmful to Democratic politicians. Weeks before the 2020 Presidential Election, the New York Post published an article, detailing the contents of a package they received.[45] Inside was a copy of Hunter Biden's hard drive containing incriminating evidence of illegal activities.[46] Twitter removed the article from its website, despite being informed by a senior FBI official that the laptop was, in fact, legitimate.[47] However, the FBI's confirmation of the laptop's legitimacy was not shared with American voters prior to the 2020 election.[48] Years later, the House Committee on Oversight and Accountability held a hearing to detail Twitter's role in suppressing the Hunter Biden laptop story.[49] During this hearing,

---

[42] *Id.*

[43] Brian Fung, *Twitter Bans President Trump Permanently*, CNN (Jan. 9, 2021, 9:19 AM), https://www.cnn.com/2021/01/08/tech/trump-twitter-ban/index.html [https://perma.cc/V7MB-847H].

[44] Vittoria Elliott, *Trump's Twitter Ban Was Unfair, But Not for the Reason You Think*, WIRED (Dec. 16, 2022, 11:49 AM), https://www.wired.com/story/twitter-trump-world-leaders-ban/ [https://perma.cc/57WR-FDNE].

[45] Farnoush Amiri & Barbara Ortutay, *Ex-Twitter Execs Deny Pressure to Block Hunter Biden Story*, AP NEWS (Feb. 8, 2023, 3:43 PM), https://apnews.com/article/technology-politics-united-states-government-us-republican-party-business-6e34ad121a1e52892b782b0b7c0e59c3 [https://perma.cc/2C3T-9N4V].

[46] *See id.*

[47] Steven Nelson, *FBI Told Twitter Hunter Biden Laptop Was Real on Day of Post Scoop, Official Says*, N.Y. POST (July 21, 2023, 3:08 PM), https://nypost.com/2023/07/20/fbi-told-twitter-hunter-biden-laptop-was-real-day-of-post-scoop-official-says/ [https://perma.cc/QT9Z-YHB8].

[48] *Id.*

[49] Press Release, H. Comm. on Oversight and Accountability, The Cover Up: Big Tech, the Swamp, and Mainstream Media Coordinated to Censor Americans'

former Twitter employees admitted that the article was taken down, despite not violating any of Twitter's policies.[50] Emails between Twitter employees on the day of the story's publication were particularly damning, with one message reading, "[i]t isn't clearly violative of our hacked materials policy, nor is it clearly in violation of anything else."[51]

However, research conducted by NYU's Stern Center for Business and Human Rights raises doubts about the legitimacy of conservatives' censorship concerns.[52] The study, analyzing interactions measured by likes, shares, and comments on politicians' Facebook pages, found that "Trump dominated Biden in Facebook Engagement."[53] In over a two-month span, the two politicians received over 307 million interactions—with Trump receiving 87%.[54] The study also measured interactions of major media providers' Facebook pages, such as Fox News, ABC News, and CNN. The results found that Fox News and Breitbart, two conservative-leaning platforms, received the most interactions.[55]

Complaints of political censorship are not new to conservatives, but concerns have been growing in recent years. In 2018, the Pew Research Center found that 85% of Republicans and 62% of Democrats felt that it was likely that social media sites intentionally censor political viewpoints.[56] For Republicans, this figure rose to 90% in 2020, while for Democrats, it dropped to 59%.[57] However,

---

Free Speech, (Feb. 8, 2023), https://oversight.house.gov/release/the-cover-up-big-tech-the-swamp-and-mainstream-media-coordinated-to-censor-americans-free-speech-%EF%BF%BC/ [https://perma.cc/XQF2-V3MX].

[50] *Id.*

[51] *Id.* (internal citations omitted).

[52] PAUL M. BARRETT & J. GRANT SIMS, NYU STERN CTR. FOR BUS. & HUM. RTS., FALSE ACCUSATION: THE UNFOUNDED CLAIM THAT SOCIAL MEDIA COMPANIES CENSOR CONSERVATIVES (2021).

[53] *Id.* at 5.

[54] *Id.*

[55] *Id.* at 8.

[56] Emily A. Vogels et al., *Most Americans Think Social Media Sites Censor Political Viewpoints*, PEW RSCH. CTR. (Aug. 19, 2020), https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/ [https://perma.cc/Z65U-JMJT].

[57] *Id.*

the Florida Legislature found that "social media platforms have unfairly censored, shadow banned, de-platformed, and applied post-prioritization to Floridians."[58] This tension creates problems for passing successful anti-censorship legislation, as the parties generally disagree on whether censorship of conservatives is occurring. These repeated instances of censorship from Big Tech further explain why Florida was willing to pass legislation designed to provoke litigation.

C. The NetChoice Litigation in Florida and Texas

Shortly after Governor DeSantis signed Bill 7072 into law, NetChoice and the Computer & Communications Industry Association filed suit to enjoin the statute.[59] NetChoice contended that Bill 7072 "brazenly infringes and facially violates the First Amendment rights" of many leading American businesses.[60] Interestingly enough, NetChoice also noted that Bill 7072 "arbitrarily favor[s] popular and larger businesses like Disney and Universal Studios . . . while also irrationally targeting popular social media companies for speech restrictions."[61]

However, following immediate litigation in the wake of Bill 7072's passage, the U.S. Court of Appeals for the Eleventh Circuit partially upheld an injunction blocking Bill 7072, in *NetChoice, LLC. v. Moody.*[62] The Florida Legislature petitioned for certiorari with the U.S. Supreme Court, arguing that the Eleventh Circuit's holding conflicted with a Fifth Circuit holding involving a similar

---

[58] Brief in Opposition at 1, NetChoice, LLC v. Moody, 143 S. Ct. 744 (2023) (No. 22-393), 2022 WL 17338968.

[59] *NetChoice & CCIA v. Moody*, NETCHOICE, https://netchoice.org/unconstitutional-social-media-bill-circumvents-rights-afforded-under-the-constitution/ [https://perma.cc/8DLP-YE3Y] (last visited Nov. 14, 2023).

[60] *See id.*

[61] *See id.*

[62] NetChoice, LLC v. Moody, 34 F. 4th 1196 (11th Cir. 2022); Kalvis Golde, *Florida's Effort to Restore its Contentious Social Media Law Arrives at the Court*, SCOTUSBLOG (Oct. 2, 2022, 10:10 PM), https://www.scotusblog.com/2022/10/floridas-effort-to-restore-its-contentious-social-media-law-arrives-at-the-court/ [https://perma.cc/86FG-5UG4].

Texas law.[63] House Bill 20 ("HB 20"), Texas' consumer privacy law, was passed in September 2021.[64] HB 20 made it illegal for social media companies to ban users based on their political viewpoints.[65] Like Bill 7072, it also required social media companies to publicly report information about how the companies removed content and handed down account suspensions.[66] On September 29, 2023, the U.S. Supreme Court granted certiorari for *Moody v. NetChoice, LLC* and *NetChoice, LLC v. Paxton*.[67]

Viewed within this context, the Florida Legislature's underlying motivations behind certain drafting decisions begin to take shape. In his order to enjoin Bill 7072, Judge Robert Hinkle of the U.S. District Court for the Northern District of Florida explicitly discussed the "deep partisan motivations of the Florida government" behind passing Bill 7072.[68] Writing for the court, Hinkle found that statements made by Governor DeSantis and other members of the Florida Legislature were indicative of "viewpoint-based motivation," and thus subject to strict scrutiny.[69]

The Florida Legislature itself foresaw the potential for First Amendment litigation when initially drafting Bill 7072. In a Bill Analysis and Fiscal Impact Statement, the Florida Senate observed

---

[63] NetChoice, LLC v. Paxton, 49 F. 4th 439 (5th Cir. 2022); *see* Golde, *supra* note 62.

[64] Kailyn Rhone, *Social Media Companies Can't Ban Texans Over Political Viewpoints Under New Law*, THE TEX. TRIB. (Sept. 2, 2021), https://www.texastribune.org/2021/09/02/texas-social-media-censorship-legislature/ [https://perma.cc/DR89-36BA].

[65] *See id.*

[66] Jesus Vidales, *Texas Social Media "Censorship" Law Goes Into Effect After Federal Court Lifts Block*, THE TEX. TRIB. (Sept. 16, 2022), https://www.texastribune.org/2022/09/16/texas-social-media-law/ [https://perma.cc/CZ38-KJ2R].

[67] Moody v. NetChoice, LLC, 34 F. 4th 1196 (11th Cir. 2022), *cert. granted in part*, No. 22-277, 2023 WL 6319654 (U.S. Sept. 29, 2023); NetChoice, LLC v. Paxton, 49 F. 4th 439 (5th Cir. 2022), *cert. granted in part*, No. 22-555, 2023 WL 6319650 (U.S. Sept. 29, 2023).

[68] Alan Z. Rozenshtein, *The Real Takeaway from the Enjoining of the Florida Social Media Law*, LAWFARE (July 9, 2021, 1:35 PM), https://www.lawfaremedia.org/article/real-takeaway-enjoining-florida-social-media-law [https://perma.cc/3VRF-CY7X**].**

[69] NetChoice, LLC v. Moody, 546 F. Supp. 3d 1082, 1094 (N.D. Fla. 2021).

that "[b]ecause some provisions of the bill seek to restrict certain speech made by internet and social media platforms, the First Amendment protections afforded to corporate speech may be implicated."[70] These statements demonstrate the Legislature's willingness to author a statute that would test constitutional boundaries and invite litigation. Many of the arguments found in *Moody* were previously outlined in this Impact Statement. The Florida Legislature recognized that the provisions of Bill 7072 might unconstitutionally limit "political corporate speech" and be read as "unconstitutional content-based restrictions."[71] These statements demonstrate the Florida Legislature's willingness to test the waters and allow federal courts to draw boundaries in this evolving area of the law.

Comments made by Governor DeSantis following the lawsuit confirm the Legislature's willingness to engage in impact legislation. In an interview prior to the passage of the FDBR, DeSantis acknowledged that Bill 7072 was designed to provoke litigation and potentially be contested all the way to the U.S. Supreme Court.[72] The Governor noted that the Bill "created the exact conflict [that] we predicted would happen," but he conceded that it was "going to be a tough case at the Supreme Court."[73]

III. UNDERSTANDING THE APPLICABILITY PROVISION LANDSCAPE

After being codified into law, critics highlighted the FDBR's narrow applicability provision and raised concerns that it would limit the bill's effectiveness. The focal point of this criticism focused on the statute's two-prong applicability test. The Florida law only regulates companies that (1) make more than $1 billion in gross annual revenue *and* (2) do any one of the following: (i) derive at

---

[70] Staff of Fla. S. Comm. on Governmental Oversight and Accountability, SPB 7072 (2021) Staff Analysis 22 (Apr. 5, 2021) (on file with Florida Senate).

[71] *Id*.

[72] *See* Sam Sachs, *DeSantis Announces 'Digital Bill of Rights' Legal Proposal for Florida*, WFLA (Feb. 15, 2023, 2:27 PM), https://www.wfla.com/news/politics/desantis-florida-attorney-general-fdle-commissioner-to-speak-in-west-palm-beach/ [https://perma.cc/C2C3-XGQS].

[73] *Id.*

least 50% of their global gross revenue from the sale of online advertising, (ii) operate a smart-speaker and voice-command service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation, or (iii) operate an app store or a digital distribution platform that offers at least 250,000 applications for consumers to download.[74]

The first prong, which limits the FDBR's applicability to only companies whose gross annual revenue exceeds $1 billion, differs significantly from other state data privacy statutes.[75] Rather than determining applicability by revenue, most state data privacy statutes determine applicability by the number of users' data a company processes in a calendar year.[76] In short, the FDBR's applicability provision prioritizes curtailing consumer data collection from large technology companies at the expense of making the statute inapplicable to smaller corporations.[77]

However, the Florida Legislature's focus on Big Tech blinded them to the obvious: that lowering the FDBR's gross annual revenue provision to include smaller companies would not disqualify companies like Meta and Amazon. For example, a gross revenue provision set more akin to Utah's Consumer Privacy Act ("UCPA"),[78] which applies to companies with a gross annual revenue exceeding $25 million, would still capture social media giants like Meta and Google.[79] Both Florida and Utah's statutes limit applicability to small businesses, yet the UCPA's gross annual revenue requirement is one-fortieth of Florida's.[80]

---

[74] FLA. REV. STAT. § 501.702(9)(a)(1)-(6) (2023).

[75] Skye Witley, *DeSantis Takes Swing at Big Tech in New Florida Privacy Law*, BL (June 6, 2023, 12:28 PM), https://news.bloomberglaw.com/privacy-and-data-security/florida-enacts-privacy-law-that-takes-a-big-swing-at-big-tech [https://perma.cc/5U4K-RLRM].

[76] *See id.*

[77] *See id.*

[78] UTAH CODE ANN. § 13-61 (2022) (effective Dec. 31, 2023).

[79] *Id.* § 13-61-102(1)(b) (2022); *see also Utah Consumer Privacy Act (UCPA): An Overview*, USERCENTRICS (Dec. 15, 2022), https://usercentrics.com/knowledge-hub/296tah-consumer-privacy-act-ucpa/#:~:text=Unlike%20some%20other%20data%20privacy,data%20is%20collected%20and%20processed [https://perma.cc/SX5V-3NJX].

[80] *See* UTAH CODE ANN. § 13-61-102(1)(b) (2022) (effective Dec. 31, 2023).

It can be difficult to differentiate between companies with a gross annual revenue of $1 billion versus those with $25 million in the abstract. To provide benchmarks, Florida's statute would not include companies like dating app, Bumble; technology giant, Blackberry; and mobile payment operator, Squarespace.[81] There is a strong policy argument that these companies should be subject to the FDBR solely based on the sensitive data that they handle. Other well-known companies, such as Hims & Hers Health, Trivago, and 23andMe, also operate with sensitive consumer information, such as reproductive health information, genetic information, and travel history, and will not be required to comply with the FDBR because of the gross revenue requirement.[82] Compared to other states, the FDBR's narrow applicability will result in weaker consumer data protections for Floridians.

A. The California Model: Pioneering State Consumer Privacy Laws

The California Consumer Rights Act, later amended to become the California Privacy Rights Act (the "CPRA"), was the first comprehensive state data privacy law enacted, and contained an extensively broad applicability provision. The CPRA outlines three distinct avenues for application.[83] A company qualifies if (1) it has a gross annual revenue exceeding $25 million; (2) it processes the personal information of 100,000 consumers annually; or (3) it derives 50% or more of its annual revenue from the sale or sharing of consumers' personal information.[84] As the first state-enacted consumer privacy law, the CPRA served as a model for state legislatures. Interestingly, most states who enacted data privacy laws after California limited applicability by *either* the annual total consumer data processed or the company's gross annual revenue. Compared to other state data privacy statutes, the CPRA's applicability provision is decidedly the most expansive to date.

---

[81] *Top Publicly Traded Tech Companies by Revenue*, COMPANIESMARKETCAP, https://companiesmarketcap.com/tech/largest-tech-companies-by-revenue/?page=4 [https://perma.cc/CP5Q-LMZZ] (last visited Oct. 1, 2023).

[82] *Id.*

[83] CAL. CIV. CODE §§ 1798.140(d)(1)(A)-(C) (2022).

[84] *Id.*

B. The Virginia Model: The Majority Approach

The Virginia Consumer Data Protection Act ("VCDPA"), the second state consumer privacy law passed, dictates applicability based on the amount of personal consumer data that a company processes annually.[85] The VCDPA applies to entities that (1) process the personal data for at least 100,000 consumers annually; or (2) process the personal data of 25,000 consumers annually and derive greater than 50% of their gross annual revenue from the sale of personal consumer data.[86] The VCDPA borrows directly from prongs two and three of the CPRA's applicability provision.

However, it departs from the CPRA in one crucial respect. Unlike the CPRA, the VCDPA's applicability section does not include a gross annual revenue-dependent applicability provision. Rather, the VCDPA considers gross revenue as one element of a two-part test, which still requires that a company process a minimum number of consumers' personal data annually to be subject to the VCDPA. States that have adopted the Virginia Model often adjust the consumer requirement to further expand or limit applicability. The Montana Consumer Data Privacy Act ("MTCDPA"),[87] for example, follows the Virginia model, but further broadens applicability to include entities that process the data of at least 50,000 Montana residents.[88]

C. The Nevada Model: Consumer-Oriented Legislation

The Nevada Online Privacy Protection Act ("NOPPA"),[89] contains a broader applicability provision, where an entity must only (1) own and operate a website for business purposes; (2) collect and maintain personal information from consumers who reside in Nevada and use or visit the website; and (3) purposefully direct

---

[85] VA. CODE ANN. § 59.1-576(A) (2023).

[86] *Id*.

[87] MONT. CODE ANN. § 30-14-NEW-001 (2023) (effective Oct. 1, 2024).

[88] *Id*. § 30-14-NEW-003(1) (2023); *see also* F. Paul Pittman et al., *Montana Joins the Growing Number of States with a Comprehensive Data Privacy Law*, WHITE & CASE (June 23, 2023), https://www.whitecase.com/insight-alert/montana-joins-growing-number-states-comprehensive-data-privacy-law [https://perma.cc/VK7Q-DX9Q].

[89] NEV. REV. STAT. § 603A (2023).

activities, transact with, or avail itself to Nevada or its citizens.[90] NOPPA captures the vast majority of companies, which, on its face, might seem appealing from a consumer protections perspective. However, becoming and remaining compliant with consumer data privacy legislation can be a costly—and potentially fatal—reality for small and medium-sized businesses. These costs include hiring chief privacy officers and privacy and compliance consultants. Soumendra Mohanty, a chief strategy officer for data analytics company, Tredence, observed that depending on the industry, the costs of maintaining compliance can reach into the tens of millions, "yet non-compliance can quickly double those numbers."[91] The fear of damaging small businesses provide a reasonable argument for adopting some variation of either the California or Virginia models in order to limit the statute's applicability to companies that are able to comply.

Crucially, however, none of these models limit the application of their consumer privacy laws solely by a company's gross annual revenue like the FDBR; rather, they all include provisions which limit applicability based on the number of people whose personal data was processed by that company. Because Florida was one of the earliest states to implement comprehensive data privacy legislation, and because the majority of the FDBR has yet to come into effect, the Legislature has a window for amending the FDBR.

IV. THE REPERCUSSIONS OF TARGETING BIG TECH

The majority of the FDBR takes effect on July 1, 2024.[92] However, embedded in the FDBR is a "unique provision" intended to prevent moderation on social media by government employees.[93] Under section 112.23, "[a] governmental entity may not

---

[90] *Id*. § 603A.100 (2023); *see also* Donata Stroink-Skillrud, *Nevada Revised Statutes Chapter 603A Compliance Guide*, TERMAGEDDON (June 22, 2022), https://termageddon.com/nevada-revised-statutes-chapter-603a/ [https://perma.cc/64PQ-2JP7].

[91] Sri Krishna, *Data Privacy is Expensive – Here's How to Manage Costs*, VENTUREBEAT (Oct. 18, 2022, 12:00 PM), https://venturebeat.com/security/data-privacy-is-expensive-how-to-manage-costs/ [https://perma.cc/VH3X-WB7A].

[92] *See* Pittman et al., *supra* note 18.

[93] *See id.*

communicate with a social media platform to request that it remove content or accounts from the social media platform."[94] This provision, unlike the rest of the FDBR, became effective on July 1, 2023.[95] Critics have argued that this provision arose from the Legislature's concerns regarding the removal of conservative media, specifically information related to COVID-19 and the 2020 election.[96] In practicality, section 112.23 bears no relation to protecting consumers' online data. The FDBR's limited scope and the longstanding feud with Silicon Valley social media companies raise legitimate questions of whether the FDBR, in its current form, could seriously be considered to protect consumer data.

A. The Relationship Between Bill 7072 and the FDBR

There is a strong argument that the Florida Legislature recognized the national trend of states passing data privacy laws and drafted the FDBR as a legislative vehicle for supplementing Bill 7072 for their continued fight with Big Tech. Leni Morales makes a highly compelling, parallel argument about the role of the Eleventh Circuit's decision in the Texas Legislature's drafting of HB 20:

> This injunction and opinion . . . no doubt helped shape the wording and direction of the HB 20 as SB 7072 and the decided unconstitutionality of the law hinged on the fact that the law was clearly content-based and aimed at protecting Florida politicians. HB 20 steered clear of the protections strictly for politicians, and aimed at the entirety of Texas, thereby hoping to clear the content-based hurdle that the Eleventh Circuit already ruled as unconstitutional.[97]

When drafting the FDBR, Florida had access to published decisions by both the Fifth and Eleventh Circuits outlining which elements of their respective anti-censorship laws were unconstitutional. More importantly, this allowed the legislature to

---

[94] FLA. REV. STAT. § 112.23(2) (2023).

[95] *See id.*

[96] *See* Jonathan Greig, *With 'Big Tech' in DeSantis' Crosshairs, Florida Becomes 10th State with Data Privacy Law*, THE REC. (June 6, 2023), https://therecord.media/florida-data-protection-law-desantis-big-tech [https://perma.cc/H75C-UY6L].

[97] Leni Morales, *Texas' War on Social Media: Censorship Or False Flag*, 33 DEPAUL J. ART, TECH. & INTELL. PROP. L. 1, 10 (2023) (footnote omitted).

tailor the FDBR's anti-censorship provisions to avoid causing challenges to their constitutionality.

In early 2023, while Florida litigated *Moody*, Governor DeSantis spoke frequently to the shared purpose of Bill 7072 and the FDBR.[98] DeSantis described Bill 7072 as part of a larger "Big Tech Crackdown."[99] His statements provoked political commentators to note that "[h]is proposals are similar to the controversial 2021 law [Bill 7072] . . . that sought to crack down on social media censorship."[100] DeSantis himself has seemingly acknowledged the relationship between the two statutes. On one such occasion, while speaking at an event focused on promoting the FDBR, DeSantis began an FDBR-focused press conference with an extensive discussion of Bill 7072 and its role as the beginning of Florida's legislative efforts against Big Tech.[101]

These comments mirrored statements from DeSantis following the passage of the FDBR. During the press conference announcing the passage of the FDBR, he stated that "[w]e want to make sure that we're providing protection to Floridians to speak their mind on these platforms, . . . [to make] sure that government is not colluding with these companies to stifle speech, like we've seen in recent history."[102] These statements serve as another indicator that Bill 7072 and the FDBR were part of a larger, more expansive crackdown on Big Tech.

B. Understanding the Need for Consumer Data Privacy Legislation

The concern that companies will play fast and loose with consumers' personal information has driven states to pass

---

[98] *See* Sachs, *supra* note 71.

[99] *Id.*

[100] Anna Wilder, *DeSantis Proposes Crackdown on Tech Companies*, POLITICOPRO (Feb. 15, 2023, 9:23 PM), https://subscriber.politicopro.com/article/2023/02/desantis-proposes-crackdown-on-tech-companies-00083160 [https://perma.cc/4XEH-VVL8].

[101] *See* Sachs, *supra* note 71.

[102] Brenda Argueta, *Florida Gov. Ron DeSantis Signs 'Digital Bill of Rights' Into Law. Here's What That Means*, CLICKORLANDO (June 6, 2023, 3:16 PM), https://www.clickorlando.com/news/politics/2023/06/06/florida-gov-desantis-holds-bill-signing-in-wildwood-heres-whats-expected/ [https://perma.cc/RQ98-UM25].

comprehensive data privacy legislation. However, state legislators must balance consumer privacy concerns with the value of consumer data to modern businesses.[103] Companies collect and leverage consumer data to develop data-driven understandings of their clients, which in-turn, allows companies to develop marketing strategies based on consumer behavior.[104] Thus, state legislators are left in the unenviable position of "treading the line between protecting citizens' privacy while facilitating technological growth."[105] The FDBR, in its current form, does not strike such a balance.

Prior to passing the FDBR, Florida legislators discussed their intent for the bill to directly address "the largest and most common [social media] platforms."[106] In a press conference held in February 2023, months prior to the bill's enactment, Governor DeSantis specifically listed Meta and Google as companies that the FDBR was intended to target.[107]

Large technology companies are by no means the only entities collecting consumer data, but the FDBR ignores that fact in a manner that harms Florida residents. A 2022 study found that 35% of businesses with an annual revenue of $50,000 or less and 40% of businesses with a revenue between $50,001 and $200,000 used

---

[103] *See* Harrison Enright, *What A Data Privacy Law Should Look Like in West Virginia: Balancing Competing Interests of Consumers and Businesses*, 125 W. VA. L. REV. 263, 265 (2022).

[104] *See* Sydney Wolofsky, *What's Your Privacy Worth on the Global Tech Market? Weighing the Cost of Protecting Consumer Data Against the Risk That New Legislation May Stifle Competition and Innovation During This Global, Technological Revolution*, 44 FORDHAM INT'L L.J. 1149, 1151 (2021).

[105] *See id.* at 1150.

[106] Lawrence Richard, *Gov. DeSantis Announces Digital Bill of Rights to Protect Floridians from Big Tech Surveillance, Censorship*, FOX NEWS (Feb. 26, 2023, 3:27 AM), https://www.foxnews.com/politics/desantis-announces-digital-bill-rights-protect-floridians-big-tech-surveillance-censorship [https://perma.cc/3HHV-FCJ8].

[107] *Id.*

consumer data for their business decisions.[108] As the survey revealed,

> [t]he most useful tidbits of information, according to business owners, were a customer's purchase history and their interaction with the business website (engagement data). Some companies, especially in the 51 to 100 employee range, were particularly interested in perhaps improving their customer database, as they focused on gathering data like their consumers' names, gender, and occupation.[109]

Crucially, these categories of consumer data are explicitly the types the FDBR intended to limit collection of.[110] Moreover, 28% of the data collected from social media was classified as "demographic analytics."[111] The study confirms what is already known: that companies of all sizes are collecting and leveraging personal consumer data to drive business success.

The Florida Senate Rules Committee heard testimony to this effect prior to passing the FDBR.[112] The Connected Commerce Council, who spoke before the Senate Committee, highlighted a survey which found that 99% of Florida's small businesses believe that "targeted digital advertising 'is more effective and less expensive than billboards, television, newspapers and radio.' "[113] Jon Potter, who represented the Connected Commerce Council, testified that targeted advertising helps small businesses "compete against larger businesses" and that the FDBR would cause small

---

[108] *Data Collection: A Business's Best Friend*, SKYNOVA, https://www.skynova.com/blog/small-business-big-data [https://perma.cc/5PXY-3HME] (last visited Nov. 13, 2023).

[109] *Id.*

[110] *See generally* FLA. REV. STAT. § 501.702(4) (2023) (" 'Biometric data' means data by automatic measurements of an individual's biological characteristics. The term includes . . . characteristics used to identify a specific individual."); *see also* FLA. REV. STAT. § 501.171(1)(g)(1) (2023) (" 'Personal information' means either of the following . . . [a]n individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual.").

[111] *See Data Collection: A Business's Best Friend*, s*upra* note 108.

[112] Mary Ellen Klas, *Florida Advances 'Digital Bill of Rights' Aimed at Big Tech*, GOVERNING (April 25, 2023), https://www.governing.com/security/florida-advances-digital-bill-of-rights-aimed-at-big-tech [https://perma.cc/EPV6-KRAQ].

[113] *Id.*

businesses to "lose money in profits . . . to pay more for advertising that doesn't work as well."[114] Alexander Fedorowicz, a co-founder and CEO for a small, 18 person skincare company based in Florida echoed these sentiments to the Rules Committee, noting that online advertising allows his company to "compete against very large companies like the Procter and Gambles and L'Oreals of this world."[115]

While large technology companies, such as Google and Meta, dominate the headlines when data indiscretions are revealed, the same cannot be said for small- and medium-sized businesses. A 2019 survey conducted by Kaspersky, a data protection company servicing small, medium, and large businesses, found that 36% of small and 48% of medium-sized businesses reported a data breach within the year.[116] Of these companies that suffered a data breach, 28% conceded that they lacked "appropriate IT solutions," and 25% of the small businesses surveyed used a "home version" of relevant security software due to prohibitively high costs.[117]

Smaller businesses are even more vulnerable because they are viewed as "softer targets" due to their limited budgets and expertise.[118] Large, sophisticated technology companies typically have the resources to remain compliant with current data privacy legislation; yet, the same cannot be said for smaller businesses dealing with consumer data.[119] The cost of storing consumer data

---

[114] *Id.*

[115] *Id.*

[116] Kaspersky defines a small business as less than fifty employees, and a medium sized business as less than 999 employees. *See Beware Being Breached: Why Data Protection is Vital for Small Businesses*, KASPERSKY, https://www.kaspersky.com/blog/data-protection-for-smb/ [https://perma.cc/Y79L-ZP5R] (last visited Nov. 13, 2023).

[117] *See id*; *see also* DIGITAL, *51% of Small Business Admit to Leaving Customer Data Unsecure* (last updated Mar. 21, 2022), https://digital.com/51-of-small-business-admit-to-leaving-customer-data-unsecure/ [https://perma.cc/V6PT-B9A2] (finding that fifty-one percent of small businesses did not have cybersecurity measures in place; moreover, that fifty-nine percent of those without cybersecurity measures did so because they considered their business "too small" to be a target of cyberattacks).

[118] *See id.*

[119] *See id.*

properly and recruiting data compliance experts to avoid running afoul of federal and state laws presents a significant barrier for small businesses.[120] The Legislature seemed to drastically underestimate this fact when drafting their applicability provisions within the FDBR.

V. MOODY V. NETCHOICE, LLC: REVIEWING BILL 7072

On September 30, 2023, the U.S. Supreme Court granted certiorari to *Moody v. NetChoice, LLC*, with oral arguments to be heard in the coming months.[121] The scope of review will be limited to two of the four questions that the U.S. Solicitor General presented: (1) whether each of the statute's content moderation restrictions violate the First Amendment; and (2) whether the statute's individualized-explanation requirements comply with the First Amendment.[122] Interestingly, despite using the Solicitor General's questions to outline the Court's scope of review, the Court declined to hear arguments on all of the questions presented.[123]

The Supreme Court, in granting certiorari for both *Moody v. NetChoice* and *NetChoice v. Paxton,* will look to clarify a circuit split between the Fifth and Eleventh Circuits.[124] In *Moody*, the Eleventh Circuit held that "S.B. 7072's content-moderation and individualized-explanation requirements likely violated the First Amendment."[125] Opposingly, in *Paxton*, the Fifth Circuit "rejected

---

[120] *See id.*

[121] Moody v. NetChoice, LLC, 34 F. 4th 1196 (11th Cir. 2022), *cert. granted in part*, No. 22-277, 2023 WL 6319654 (U.S. Sept. 29, 2023).

[122] *Id. Moody v. NetChoice, LLC*, SCOTUSBLOG, https://www.scotusblog.com/case-files/cases/moody-v-netchoice-llc/ [https://perma.cc/8XQD-L98X] (last visited Nov. 13, 2023).

[123] Moody v. NetChoice, LLC, No. 22-277, 2023 WL 6319654 (U.S. Sept. 29, 2023). *See* Brief for the United States as Amicus Curiae at 12, Moody v. NetChoice, LLC (2023) (No. 22-277), 2023 WL 6319654 (U.S. Sept. 29, 2023) ("The Court should therefore deny NetChoice's conditional cross petition in *Moody* (No. 22-293) and deny NetChoice's petition in *Paxton* to the extent it raises issues that go beyond questions one and two in this brief.").

[124] Brief for the United States as Amicus Curiae at 12, Moody v. NetChoice, LLC (2023) (No. 22-277), 2023 WL 6319654 (U.S. Sept. 29, 2023).

[125] *See id.* at 2.

key aspects of the [Eleven]th Circuit's analysis of the content-moderation and individualized-explanation provisions."[126]

The U.S. Solicitor General's amicus brief provides a roadmap of the direction of the *Moody* litigation. The Solicitor General argued that the U.S. Supreme Court should affirm the Eleventh Circuit and reverse the Fifth Circuit.[127] The brief notes that the 11th Circuit's decision should be affirmed because "the individualized-explanation requirements impose heavy burdens on the platforms' expressive activities that the States have failed to justify."[128] Fundamentally, Bill 7072's individualized-explanation provisions—located in section 501.2041(3)(c)-(d)—aim to hold social media companies accountable for their content removal decisions.[129] Thus, the Florida law required "platforms to provide an individualized explanation each time they exercise[d] editorial discretion by removing user content."[130]

The U.S. Solicitor General took the position that the "sheer volume of content removal" that social media platforms undertake presents a significant issue for Florida's individualized-explanation requirements.[131] During this litigation, Florida has presented two primary arguments in defense of the provisions: (1) that content moderation is not protected speech; or alternatively, (2) that even if content moderation is protected speech, "requiring individualized explanations is not unduly burdensome."[132] However, based on the Solicitor General's amicus brief and the Eleventh Circuit's holding in *Moody*, these arguments seem unlikely to succeed. If so, Florida will need to consider new strategies for holding Big Tech accountable for content removal without triggering future litigation. However, a suitable replacement might already lie in Bill 7072's companion statute: Texas' HB 20.

---

[126] *See id.* at 3.

[127] Brief for the United States as Amicus Curiae at 18, Moody v. NetChoice, LLC (2023) (No. 22-277), 2023 WL 6319654 (U.S. Sept. 29, 2023).

[128] *Id.* at 18-9.

[129] *Id.* at 19.

[130] *Id.*

[131] *See id*.

[132] *Id*.

VI. LEGISLATIVE RECOMMENDATIONS

Irrespective of political motivations, the FDBR represents a partial victory for the data privacy rights of Floridians. After stripping away the partisan motivations behind the FDBR, Floridians are left in a unique situation. On the one hand, Florida was an early mover in enacting comprehensive state data privacy legislation that complements federal data privacy statutes. On the other hand, the Florida Legislature's intent on drafting a statute aimed at harming large companies like Amazon and Meta resulted in a law with limited applicability. The Florida Legislature, in serving its constituents, would be prudent to consider amending the FDBR to better reflect its constituents' interests.

This Article provides legislative recommendations in two respects: (1) revisions addressing personal consumer privacy-related concerns, and (2) revisions for the FDBR based on the upcoming ruling in *Moody v. NetChoice, LLC*. Firstly, Florida should amend the FDBR to either remove the gross annual revenue requirement entirely or broaden the FDBR's applicability provision by lowering the gross annual revenue requirement to a figure more comparable with other jurisdictions. Second, following the *Moody* decision, the Florida Legislature should incorporate any Bill 7072-related amendment into the FDBR. After touting the statute as Florida's comprehensive Bill of Rights for digital matters, the Legislature would bolster the FDBR's legitimacy by expanding the statute. Third, the Legislature should follow the guidance provided by the U.S. Supreme Court in *Moody* in conjunction with considering potential amendments based on Texas' HB 20.

A. Amending the FDBR's Gross Annual Revenue Requirement

If Florida intends to continue curtailing Big Tech, it should do so without risking the sensitive consumer data of its constituents. Small and medium-sized companies are increasingly relying on consumer data to inform business decisions—except, that they will likely collect, maintain, and sell this data with a lower level of security and sophistication than their larger counterparts.[133] Florida should join the view shared by other state legislatures—which

[133] *See* DIGITAL, supra note 117.

include the historically Democratic California with the traditionally Republican Texas—that online consumer privacy is a threat worth taking seriously from companies of all sizes.

Of the thirteen states to pass data privacy legislation, only three include a gross annual revenue requirement in their applicability provisions. Both Utah and Tennessee have set their gross revenue requirement at $25 million—a figure significantly lower than Florida's.[134] When compared with other jurisdictions, there is little debate that the FDBR's gross annual requirement was set abnormally high. A cognizable reduction, aligning with both Utah and Tennessee, would be to lower the gross annual revenue requirement to $25 million. Alternatively, Florida's revisions could follow the Virginia model, which determines applicability by the number of state residents whose data the company processes each year.[135] Following the Virginia model, as the current majority approach, would provide a benefit to Florida businesses by easing their compliance burdens. Crucially, either revision can be tailored to broadly capture both large technology companies and smaller businesses.

These concerns were echoed by Matt Schwartz, a policy analyst for Consumer Reports. Schwartz's concern, that the FDBR would not apply to most online platforms, highlights the limitations accepted by the Florida Legislature at the expense of Floridians' consumer privacy. As he described, "[t]his legislation's narrow applicability means that most products and services consumers encounter online, including the vast majority of app[lications], will not need to follow these new privacy standards."[136] As another

---

[134] UTAH CODE ANN. § 13-61-102(1)(b) (2022) (effective Dec. 31, 2023); TENN. CODE ANN. § 47-18-3202(1) (2023) (effective July 1, 2025). *See* F. Paul Pittman et al., *Tennessee Passes Comprehensive Data Privacy Law*, WHITE & CASE (June 23, 2023), https://www.whitecase.com/insight-alert/tennessee-passes-comprehensive-data-privacy-law [https://perma.cc/E6CD-BNW3].

[135] *See* VA. CODE ANN. § 59.1-576(A) (2023); *see also* F. Paul Pittman et al., *Virginia Joins California in Regulating Consumer Information: Virginia Enacts the Consumer Data Protection Act*, WHITE & CASE (Mar. 5, 2021), https://www.whitecase.com/insight-alert/virginia-joins-california-regulating-consumer-information-virginia-enacts-consumer [https://perma.cc/YJ98-6GJ4].

[136] Matt Schwartz, *Consumer Reports Calls on Florida to Strengthen Newly Passed Privacy Legislation*, CONSUMER REPS. (May 5, 2023),

commentator described, "the revenue requirement means that Floridians [sic] will not receive new rights or protections with respect to the vast majority of businesses that collect their personal data in the Sunshine State."[137]

However, while Florida should lower the FDBR's gross revenue requirement, it does not need to lower it to match Utah and Tennessee at $25 million annually. Initially, Florida's Rules Committee proposed a significantly broader applicability statute but was met with concerns from Florida's small business owners.[138] This caused the Committee to rewrite the bill to "limit the scope to the tech giants."[139] The Miami Herald reported that after this rewrite, "[t]he House Commerce Committee did not amend its proposal, but passed it with little discussion."[140] In balancing consumer interests against those of small business owners, the Legislature responded too strongly in favor of small businesses. Because of the rapid evolution of state consumer privacy laws, Florida should consider a compromise.

While settling on an exact figure would require further research into the advertising habits of Florida's small businesses and the likely effects of lowering the FDBR's revenue requirement, the Legislature should view $200 million as a reasonable starting point. An applicability provision in the mid-to-low nine figures would represent a significant departure from all previous state privacy statutes. To limit FDBR applicability to companies with $200 million of gross annual revenue would be eight times higher than the privacy statutes passed by Utah and Tennessee—a fact which should mitigate outcries from Florida's small businesses. For consumers, such an amendment would provide significantly stronger protections than currently exist.

---

https://advocacy.consumerreports.org/press_release/consumer-reports-calls-on-florida-to-strengthen-newly-passed-privacy-bill/ [https://perma.cc/LD4S-LKVL].

[137] Tatiana Rice et al., *Shining a Light on the Florida Digital Bill of Rights*, FUTURE PRIV. F. (May 18, 2023), https://fpf.org/blog/shining-a-light-on-the-florida-digital-bill-of-rights/ [https://perma.cc/V69B-6RXR].

[138] *See* Klas, *supra* note 112.

[139] *Id.*

[140] *Id.*

In no uncertain terms, the FDBR cannot function as promised without significantly more companies being required to comply. The Florida Legislature's misstep was not to engage in a legislative feud with large technology companies, but rather, that the Rules Committee's response overly weakened a law designed to shield Floridian's private information. Regardless of their concerns with Silicon Valley, Florida must recognize that data privacy has become an issue of significance and cannot simply be treated as another avenue to air the Legislature's grievances with a political foe. However, in the same breath, Florida should not unduly burden its business owners by following states like Utah or Tennessee. Only one issue of importance for the Legislature remains: finding a gross annual revenue figure between $25 million and $1 billion that meets those objectives simultaneously.

B. Refining the Digital Bill of Rights Anti-Censorship Provisions

The U.S. Supreme Court's decision to grant certiorari provides Florida with an opportunity to defend the law and possibly amend their anti-censorship provisions to reflect the Court's ruling. Both Bill 7072 and elements of the FDBR were explicitly drafted to address viewpoint discrimination and censorship against politicians. During the debates over Bill 7072, many Republican representatives argued that they and their constituents had been "banned or de-platformed on social media sites."[141] It is not surprising, then, that the Florida Legislature included section 112.23 in the FDBR. However, it changed its approach after the appellate court's ruling in *Moody*. Rather than drafting a law that prevents social media companies from acting in particular ways, section 112.23 focuses solely on the actions of government employees.

The U.S. Supreme Court's upcoming decision in *Moody v. NetChoice, LLC* will clarify the extent of "[s]tates' authority to restrict a business's ability to select, edit, and arrange the third-party

---

[141] David McCabe, *Florida, in a First, Will Fine Social Media Companies That Bar Candidates*, N.Y. TIMES (May 24, 2021), https://www.nytimes.com/2021/05/24/technology/florida-twitter-facebook-ban-politicians.html [https://perma.cc/ZWY8-C23C].

content that appears on its social-media platform."[142] The importance of the details underlying this forthcoming decision cannot be understated for the purposes of the FDBR. The U.S. Solicitor General, in her amicus curiae, argued that the Court should affirm the Eleventh Circuit.[143] If the Supreme Court's decision in *Moody* provides an avenue for legislating against content moderation, Florida would be wise to amend the FDBR to reflect the Court's order.

The U.S. Solicitor General's amicus brief provides insight into the key provisions under review and guidance toward a potential U.S. Supreme Court decision. The Solicitor General observed that "the content-moderation restrictions of S.B. 7072 . . . are not general regulations of conduct that only incidentally burden speech; instead, the laws are '*directed at* the communicative nature' of the major platforms' editorial activities."[144] Section 112.23 of the FDBR, on its face, seems to fall directly within that scope, where provisions such as section 112.23(2)[145] read as "general regulations of conduct" rather than being targeted at limiting social media platforms' editorial activities.[146]

The Court's decision to review Bill 7072 and HB 20 in tandem provide the opportunity for Florida to identify anti-censorship provisions in HB 20 deemed constitutional and potentially adopt them. For example, section 120.053 of HB 20 requires a bi-annual transparency report to be published by a social media platform.[147] Specifically, section 120.053(2) requires that this biannual report include "the number of instances in which the social media platform took action with respect to . . . potentially policy violating content."[148] Section 120.053(2)(A)-(G) clarifies what actions must

---

[142] Brief for the United States as Amicus Curiae at 12, Moody v. NetChoice, LLC (2023) (No. 22-277), 2023 WL 6319654 (U.S. Sept. 29, 2023).

[143] *See id.* at 13.

[144] *See id.* at 16.

[145] TEX. BUS. & COM. CODE § 120.053(2) ("[A government entity may not communicate with a social media platform to request it remove content or accounts from the social media platform.").

[146] FLA. REV. STAT. § 501.2041(1)(b) (2021).

[147] TEX. BUS. & COM. CODE § 120.053.

[148] *Id.* § 120.053(2).

be included within the biannual report, such as "content removal;" "content demonetization;" "content deprioritization;" and "account suspension."[149] To contextualize this potential amendment, adopting such a passage in the FDBR would address similar concerns first raised by Tulsi Gabbard—where content or account removal decisions are made by social media companies without providing a reasonable explanation.

The value of drafting a provision modeled after HB 20's biannual transparency requirement for the Florida Legislature becomes clearer in light of the challenge to Florida's own individualized-explanation requirement.[150] The U.S. Solicitor General, as a relatively neutral party, explained that "[g]iven the sheer number of content-moderation actions taken by the major platforms," the Eleventh Circuit found it substantially likely that Bill 7072's " 'requirement that platforms provide notice and a detailed justification' for each such action would chill 'platforms' exercise of editorial judgement.' "[151] However, because section 120.053 of HB 20 did not trigger review from the Eleventh Circuit, the Florida Legislature could seemingly adopt a similar provision without triggering further litigation. Depending on the Legislature's aptitude for further litigation, they could draft stricter provisions—requiring bi-monthly transparency reports, for example—to hold social media platforms to an even higher standard than that required in Texas.

Furthermore, while section 120.053 of HB 20 requires social media platforms to report "the number of instances," the Florida Legislature could draft a provision requiring platforms to categorize content or accounts that have been removed, demonetized, or deprioritized by *political* or *non-political* labels.[152] While defining what would make a post or account "political" requires significant thought, the Legislature might value social media platforms reporting the percentage of political content and accounts removed. Bill 7072, in its current form, requires platforms to "provide notice and detailed justifications" for each act—and early indicators

[149] *Id.* §§ 120.053(2)(A)-(G).

[150] *See* Brief for the United States as Amicus Curiae at 7, Moody v. NetChoice, LLC (2023) (No. 22-277), 2023 WL 6319654 (U.S. Sept. 29, 2023).

[151] *See id.*

[152] TEX. BUS. & COM. CODE § 120.053.

suggest that the U.S. Supreme Court will uphold the Eleventh Circuit's injunction of these provisions. However, there is a reasonable argument that requiring platforms to define political speech and subsequently categorize removed, demonetized, or deprioritized content as either political or non-political requires significantly less of these platforms and thus does not chill speech.

If, as expected, HB 20 section 120.053 remains untouched by the High Court, Florida could easily model a similar transparency report requirement provision into the FDBR. The state will have an opportunity to hear from the U.S. Supreme Court what it deems an unconstitutional chilling of social media platforms' protected editorial speech. In response, Florida may tailor a model section 120.053 provision in-line with the Supreme Court's guidelines. In most respects, it would accomplish the same objective as section 112.23 of Bill 7072—requiring companies to publish the frequency at which they remove, demonetize, or deprioritize posts and accounts. However, to accomplish their goals of requiring platforms to be transparent about political censorship, Florida would likely enact a provision requiring transparency reports from social media platforms that identify the posts or accounts that are political in nature. Yet, assuming that the U.S. Supreme Court finds that section 112.23 of Bill 7072 is unconstitutional, this provision cannot require explanations or responses that are individualized. For this reason, requiring that a platform's transparency report include statistics regarding how many of their affected posts or accounts are political in nature is a better method for achieving their goals.

VII. CONCLUSION

Florida's passage of the Digital Bill of Rights represented a partial victory for the consumer privacy protections of its residents. However, its impact remains limited, as the statute only applies to the very largest companies which collect and process consumer data. While evidence of political censorship by large technology companies continues to mount, the Legislature would be wise to recognize the repercussions for Florida's consumers by drafting the Digital Bill of Rights to exclusively target Big Tech. While the consumer privacy landscape, particularly at the state level, continues to evolve quickly, states like California, Virginia, and Tennessee

provide Florida with alternative approaches worth further consideration.

Consequently, Florida should implement the following. Firstly, Florida should amend the Digital Bill of Rights' applicability provision by lowering the gross annual revenue requirement and thus broadening applicability to a greater number of companies. Secondly, the Legislature should consolidate future Bill 7072-related, anti-censorship amendments into the FDBR to further establish and legitimize the statute as Florida's comprehensive bill of rights for technology-related legislation. Finally, Florida should consider both the *Moody* decision and Texas' HB 20 for drafting subsequent anti-censorship provisions. Adopting these amendments would bolster the FDBR and provide Floridians with actionable consumer privacy and anti-censorship protections without unduly harming Florida's small businesses.