THE FLORIDA DIGITAL BILL OF RIGHTS: PROVIDING EXPANDED CONSUMER PROTECTION IN THE DIGITAL WORLD

Veronika Balbuzanova, Esq., CIPP/US[*]

Abstract

The Florida Digital Bill of Rights comprises a statutory framework designed to regulate the use and collection of Florida consumers' personal data in the digital world. This Article breaks down the components of the new statute and explores its preliminary successes and shortcomings, particularly from an enforcement perspective.

INTRODUCTION

Effective July 1, 2024, Chapter 501 of the Florida Statutes features a brand-new statutory component that establishes consumer protections in data privacy and security—an area that has heretofore seen very little of it. The Florida Digital Bill of Rights, beginning at Florida Statute section 501.701, establishes extensive policies and procedures regulating the collection and use of consumers' personal data. While the new statute boasts laudable strengths, like establishing extensive consumer rights, the degree to which these rights will be protected and enforced is significantly undercut by the lack of a private cause of action and the narrow scope and applicability of the new law.

---

* Ms. Balbuzanova is a partner at the law firm of Johnson | Dalal in West Palm Beach, Florida. She earned her Bachelor's degree with Honors from Nova Southeastern University where she majored in Legal Studies and minored in Applied Behavior Analysis. Pursuing her love of the law, she graduated *summa cum laude* from the Shepard Broad College of Law at Nova Southeastern University with her Juris Doctorate degree. During her time at the Shepard Broad College of Law, Ms. Balbuzanova served as the Volume 43 Lead Articles Editor of Nova Law Review. She obtained her CIPP/US certification in 2023. With a passion for Data Privacy, Cybersecurity, and Social Media Law, Ms. Balbuzanova enjoys navigating the legal landscape of technology and the law while keeping clients' interests at the forefront.

I. CONSUMER RIGHTS

One of the most commendable aspects of the Florida Digital Bill of Rights is the comprehensive consumer rights that it established for Florida residents. Consumers are granted broad power and control over the collection and use of their personal data. "Personal data" is broadly defined as any information, with the exception of deidentified data or publicly available information, which is "linked or reasonably linkable to an identified or identifiable individual."[1]

A consumer is entitled to obtain confirmation as to whether a controller is processing the consumer's personal data and to access the personal data.[2] Many current data privacy concerns stem from the fact that consumers have no idea who has their personal data, what specific personal data they have, and how to go about determining this information in the first place. Not only does the new statute affirmatively grant consumers the right to access the personal data that controllers have on them, it also establishes a streamlined procedure for consumers to request that access and to exercise the other consumer rights established by the statute.[3] Specifically, consumers may submit a request to a controller specifying the consumer right(s) that the consumer wishes to exercise.[4] The controller is required to establish two or more "secure, reliable, and clearly and conspicuously accessible" methods of enabling consumers to submit a request to exercise their consumer rights.[5] In developing these methods, the controller must take into account (a) the ways in which consumers normally interact with the controller, (b) the necessity for secure and reliable communications of the requests, and (c) the ability of the controller to authenticate the identity of the consumer making the request.[6] Upon receipt, the controller must respond to the consumer request "without undue delay" and in no event later than forty-five days after receipt, though this time period may be extended by fifteen days if reasonably necessary and if specific procedures are followed.[7] The controller is also obligated to establish a process for a consumer to appeal the controller's refusal to take action on a request.[8] Not much statutory guidance is provided as to the appellate process and the obvious drawback is that the appeal, like the initial consumer request, is reviewed by the controller. Theoretically, the exact same department or representative of the controller who reviewed the consumer request may

1. FLA. STAT. § 501.702(19) (2024).
2. *Id.* § 501.705(2)(a).
3. *Id.* § 501.705(1)–(2).
4. *Id.*
5. *Id.* § 501.709(1).
6. *Id.*
7. FLA. STAT. § 501.706(2) (2024).
8. *Id.* § 501.707(1).

also be reviewing the appeal so it is unlikely that a different outcome would be reached, especially where no specific guidance is provided as to how the review of the consumer request is any different substantively from the review of the appeal. Controllers who are on the receiving end of consumer requests that are "manifestly unfounded, excessive, or repetitive" are given the option of either (1) denying the request outright or (2) charging the consumer a reasonable fee to cover the administrative costs of complying with the request.[9]

Reminiscent of the rights established under the federal Fair Credit Reporting Act, the Florida Digital Bill of Rights also creates a consumer right "[t]o correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data."[10] Notably, the statute anticipates the possibility that a controller may implement a self-service mechanism of allowing a consumer to correct certain personal data and permits a controller to deny a consumer request and require the consumer to correct his or her own personal data through this mechanism.[11] Depending how the self-service mechanism is structured and monitored, it may strike a reasonable balance between consumers' interests in correcting their personal data and controllers' interests in achieving these ends without undue burden. Given the broad definition of "personal data," that disputes may arise as to whether a consumer's personal data is, in fact, inaccurate and who the final arbiter of that inquiry is or should be—for example, with respect to personal data that the consumer claims is defamatory.

Additional consumer rights established by the statute include (1) the right to delete any or all personal data provided by or obtained about the consumer; (2) the right to obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format; and (3) perhaps most notably, the right to opt out.[12] Consumers have the right to opt out of several activities, including (a) the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer; (b) the collection of sensitive data, including precise geolocation data, or the processing of sensitive data; and (c) the collection of personal data collected through the operation of a voice recognition or facial recognition feature.[13] "Sensitive data" is a subset of personal data that includes personal data revealing an individual's racial

9. *Id.* § 501.706(5).
10. *Id.* § 501.705(2)(b).
11. *Id.* § 501.706(3).
12. *Id.* § 501.705(2)(c)–(e).
13. FLA. STAT. § 501.705(2)(e)–(g) (2024).

or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data processed for the purpose of uniquely identifying an individual; personal data collected from a known child; or precise geolocation data.[14] Though many mobile applications, websites, and digital platforms have started featuring an opt-out option, the scope and nature of the opt-out will now be subject to the foregoing requirements.

While not expressly categorized as a "consumer right," the new statute also imposes a number of duties with respect to privacy notices that create an implied consumer right to receive a full, fair, and current disclosure of a controller's data privacy practices.[15] A controller is required to furnish consumers with a "reasonably accessible and clear" privacy notice that is updated at least annually and that includes various disclosures, including what personal data is collected, what personal data is shared with third parties, for what purpose(s) the personal data is collected, and how consumers can exercise the consumer rights referenced above.[16] If a controller sells any of the consumer's sensitive data, biometric data, or personal data,[17] a clear, conspicuous, and specific notice of the same must be provided.[18]

II. APPLICABILITY

After seeing the expansive consumer rights established by the statute, consumers and practitioners alike may be surprised to discover the exceedingly narrow and limited applicability of the statute—that is, *whose* conduct the statute actually regulates. The definition of a "controller" is a key component of this statute as there are multiple conditions that must be met for an entity to qualify as a controller.

The first condition is that a qualifying controller must be a sole proprietorship, partnership, limited liability company, corporation, association, or legal entity—or any entity that controls or is controlled by a controller.[19] Individuals are excluded from the definition of a "controller." If an entity satisfies the first condition, it must then determine whether it meets the next set of lengthy criteria. Specifically, the second condition is that the entity must meet *all* of the following criteria: (1) is organized or operated for the profit or financial benefit of its shareholders or owners; (2) conducts business in this state; (3) collects personal data about consumers, or is the entity on behalf of which such information is collected; (4) determines the purposes and means of

14. *Id.* § 501.702(31).
15. *See id.* § 501.711.
16. *Id.* § 501.711(1).
17. Only personal data sold for targeted advertising is implicated. *Id.* § 501.711(4).
18. *Id.* § 501.711(2)–(4).
19. *Id.* § 501.702(9)(a)–(b).

processing personal data about consumers alone or jointly with others; and (5) makes in excess of $1 billion in global gross annual revenues.[20] If the entity meets all of the foregoing requirements, then it must determine whether it satisfies the last and final condition. The third condition is that the entity must either (a) "derive[] 50 percent or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online," *or* (b) "operate[] a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation," *or* (c) "operate[] an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install."[21]

Few entities will satisfy all of these conditions and qualify as a "controller" for purposes of the statute. The protection afforded by the Florida Digital Bill of Rights, therefore, can be quite limited given the handful of data controllers it will actually apply to and regulate. Were this a data breach notification statute, then perhaps limiting the qualifying controllers to those with significant global gross annual revenues would be a fair and reasonable restriction. But the rights and duties established by the statute should ideally apply across the board, regardless of controllers' annual revenues, because the consumer rights that are created are no less important or less fundamental when applied to a small start-up as compared to a national conglomerate. The right to access, correct, and delete one's personal data—and to be given a full and fair disclosure of a controller's privacy notice—is an unalienable right in a digital economy like the present one that is enabling controllers to financially profit off the personal data of its users. There is no doubt that the fundamental significance of these rights is what led to its compelling name—the Florida Digital *Bill of Rights*. While the statute currently maintains a narrow scope and applicability, practitioners would be well-served in treating the law's requirements as aspirational goals that all clients, regardless of their annual revenue, should strive to comport with. In time, the scope of the statute will likely be significantly broadened to align with consumers' reasonable expectations of privacy in the digital economy.

III. ENFORCEMENT

A huge drawback of the Florida Digital Bill of Rights is that it does not create a private cause of action and vests the Department of Legal

20. *Id.* § 501.702(9)(a)(1)–(5).
21. *Id.* § 501.702(9)(a)(6).

Affairs with sole enforcement authority.[22] The statute even goes so far as to state that, "liability for a tort, contract claim, or consumer protection claim unrelated to an action brought under this section does not arise solely from the failure of a person to comply with this part."[23] Although section 501.72 expressly establishes that "[a] violation of this part is an unfair and deceptive trade practice actionable under part II of this chapter", i.e., actionable under the Florida Deceptive and Unfair Trade Practices Act, consumers are essentially left without legal recourse and are wholly dependent on the Department of Legal Affairs for protection of their newly established rights and enforcement of the new statute.[24] The efficacy of the statute in policing and deterring violative conduct may, therefore, be weakened given the lack of a private cause of action.

IV. CONSENT AND LACK THEREOF

Consent is not necessarily the focal point of the statute, but a medley of statutory provisions and definitions draw significant attention to what does, and does not, amount to legally sufficient consent.

Substantial emphasis is placed on the requirement that the statutory disclosures be clear and accessible. The controller's methods of enabling consumers to submit a request to exercise their consumer rights must be "secure, reliable, and clearly and conspicuously accessible".[25] The privacy notice furnished by the controller must be "reasonably accessible and clear".[26] The process by which a controller sells or processes personal data for targeted advertising, and the manner in which a consumer may opt out of that process, must be "clearly and conspicuously disclose[d]".[27] An "up-to-date, plain language description of the main parameters that are individually or collectively the most significant in determining ranking" in search engines must be made available to consumers in an easily accessible location.[28] Notably, any measures taken to compromise the integrity of a consumer's consent are strongly spurned and prohibited. For example, a controller may offer financial incentives, including payments to consumers as compensation, for the processing of personal data "if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program and provided that such incentive practices are not unjust, unreasonable, coercive, or usurious in nature."[29] The use of dark patterns in obtaining

22. *Id.* § 501.72(1), (8).
23. FLA. STAT. § 501.72(7) (2024).
24. *Id.* § 501.72(1).
25. *Id.* § 501.709(1).
26. *Id.* § 501.711(1).
27. *Id.* § 501.711(4).
28. *Id.* § 501.71(4).
29. FLA. STAT. § 501.71(2)(c) (2024).

consent voids the consent altogether.[30] "Dark patterns" are statutorily defined as "user interface[s] designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision-making, or choice."[31] Given the Federal Trade Commission's documented rise in the use of "dark patterns" online,[32] the fact that the Florida Digital Bill of Rights declares that legally sufficient consent cannot be obtained through the use of dark patterns creates a promising foundation for the future of consumer protections. The new statute also prohibits the waiver or limitation of the consumer rights established in sections 501.705, 501.706, and 501.707 through a contract or agreement, and declares the same to be void, unenforceable, and contrary to public policy.[33]

The statute defines "consent" as "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer."[34] Consent may be given through a written statement or an "unambiguous affirmative act," but it cannot be given or inferred from a consumer "[h]overing over, muting, pausing, or closing a given piece of content."[35] Consent is also insufficient if it is part of a consumer's acceptance of general or broad terms of use or a similar document which contains descriptions of personal data processing along with other unrelated information.[36] As evidenced by the foregoing restrictions, the standard of legally sufficient consent for purposes of the Florida Digital Bill of Rights is a high one.

CONCLUSION

Adding a new consumer protection statute in the area of data privacy and security to Chapter 501 of the Florida statutory framework was a huge leap forward for the Florida Legislature. Various provisions of the statute—such as the exclusion of dark patterns from consent and the allowance for a self-serving mechanism of correcting consumer's personal data—show promise that the Florida Digital Bill of Rights will successfully keep up with technological developments in the digital world. Although the law's currently limited applicability and lack of a private cause of action suggest that there may be challenges in enforcing and protecting consumers' newly created digital rights, these are

30. *Id.* § 501.702(7)(c).

31. *Id.* § 501.702(11).

32. *Bringing Dark Patterns to Light*, FED. TRADE COMM'N (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf [https://perma.cc/QNN5-QVW2].

33. FLA. STAT. § 501.708 (2024).

34. *Id.* § 501.702(7).

35. *Id.*

36. *Id.* § 501.702(7)(a).

shortcomings that may—and hopefully will—be remedied in years to come.