NATIONAL TAXPAYERS UNION

Issue Brief

APRIL 21, 2023
BY RYAN NABIL

Florida's Recently Proposed Data Privacy Legislation Misses the Mark

Introduction

In March 2023, Florida lawmakers introduced new legislation in the state's House of Representatives and Senate focused on data privacy and certain transparency issues. Despite some differences, the Senate and the House versions of the legislation propose broadly similar rules to protect consumer privacy as well as certain measures to limit the government's role in social media content moderation and improve the transparency of search engine results related to "politically partisan" or "ideological" content.[1] The proposed law—essentially a data privacy bill combined with additional requirements for social media platforms and search engines—risks exacerbating the increasingly confusing patchwork of overlapping state and federal privacy laws and creating further uncertainties for consumers and businesses. The legislation's potential to improve Florida residents' consumer rights and statewide privacy practices across different sectors remains limited, however, as

[1] Florida House of Representatives, H.B. 1547 (2023). Retrieved from: https://www.flsenate.gov/Session/Bill/2023/1547/Bill. Florida Senate, S.B. 262 (2023). Retrieved from: https://flsenate.gov/Session/Bill/2023/262.

Key Facts:

- **Florida's recently proposed privacy law risks exacerbating the increasingly complex patchwork of overlapping federal and state privacy laws.**
- **The legislation's potential in improving statewide consumer rights and privacy practices remains limited as it would only apply to a relatively small number of companies.**
- **The proposed law's overly broad proposals related to social media platforms and search engine algorithms go far beyond the scope of any other state privacy laws.**

it would only apply to a relatively small number of companies. Furthermore, overly broad proposals related to social media platforms and search engine algorithms go far beyond the scope of other state-level privacy laws. Instead of passing poorly designed legislation at the state level, Florida lawmakers should consider focusing their efforts at the federal level, where the state could play an important role in advocating a pragmatic, principles-based privacy framework that could better balance the competing priorities of data privacy, technological innovation, and commercial needs.

Florida's Proposed Privacy Law Would Contribute to a Growing Patchwork of Overlapping Federal and State Privacy Rules

When designing a privacy framework, lawmakers must first ask what the purpose of privacy legislation is. Typically, privacy laws create a uniform set of rules by stipulating consumer rights and business obligations for public and private entities that deal with the sensitive personal data of consumers in a given jurisdiction. Ideally, a privacy framework should 1) create uniform rules based on the type of sensitive data and the way they are processed, used, or stored; 2) improve consumer awareness and confidence in how their private data is used and protected; 3) reduce data privacy and security violations; 4) lower transaction and regulatory costs; and 5) promote technological innovation. To achieve these objectives, the framework should strike the right balance between the competing objectives of data privacy and security, commercial considerations, and technological innovation. At the national level, privacy law should also contain preemption and superseding powers over conflicting federal and state statutes and harmonize rules across different sectors and states, helping create a digital single market for the whole country.

Notwithstanding the need for harmonized, comprehensible privacy rules for all businesses, the U.S. data privacy landscape is characterized by overlapping jurisdiction between multiple federal regulators and state governments, leading to a fragmented patchwork of confusing rules for startups, businesses, and consumers alike. Unlike in other major economies—such as the European Union, Japan, and China—the United States does not have a comprehensive national privacy law.[2] Instead, overlapping federal and state statutes and agency rulemaking have created divergent privacy rules that vary according to the sector of covered entities, the type and scope of business activities, and the state(s) where businesses and their consumers are located, among others.[3]

At the federal level, at least a dozen statutes provide the legal framework for privacy rules aimed at entities in different sectors, ranging from education to financial services to healthcare (Table 1). Some of these rules apply to different industries while others apply to distinct commercial activities within the same broad sectors, such as financial services. For example, the Gramm-Leach-Bliley Act imposes certain data protection obligations related to nonpublic personal information on financial institutions, while the Fair Credit Reporting Act lays out rules related to the collection and use of information for credit reporting purposes (Table 1). Meanwhile, federal securities laws have established certain disclosure requirements related to data breaches for public companies (Table 1). These statutes have also created a complex division of regulatory and enforcement powers, sometimes divided between different federal and state regulators. As a result, even at the federal level, the U.S. privacy regime appears increasingly more complicated compared to that of the European Union, which has managed to create more uniform and predictable rules across different sectors and member states that vary widely in their legal systems and historical approaches to consumer privacy.[4]

[2] Regulation EU 2016/679 (The General Data Protection Regulation). Chinese Personal Information Protection Law (2021). The Japan Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2020).
[3] For a longer discussion, see Mulligan, Stephen P., Freeman, Wilson C., and Linebaugh, Chris D. "Data Protection Law: An Overview." Congressional Research Service R45631, March 25, 2019. Retrieved from: https://sgp.fas.org/crs/misc/R45631.pdf.
[4] Regulation EU 2016/679.

Table 1. Overview of U.S. Federal Laws with Privacy Implications		
Legislation	**Brief Description and Scope of Privacy Rules**	**Agency with Civil Enforcement Authority**
Gramm-Leach-Bliley Act (GLBA) (1999)	Consent, disclosure, and data security requirements related to "nonpublic personal information" for financial institutions	Consumer Financial Protection Bureau, Federal Trade Commission, federal banking agencies
Health Insurance Portability and Accounting Act (HIPAA) (1996)	Consent, disclosure, data security, and data breach disclosure requirements related to "protected health information" for healthcare providers, health plans, and healthcare clearinghouses	Department of Health and Human Services
Fair Credit Reporting Act (FCRA) (1970)	Certain requirements related to the collection and use of consumer information by credit reporting agencies (CRA), CRA users, and data providers	Federal Trade Commission and Consumer Financial Protection Bureau; each agency has enforcement authority over entities under their respective jurisdiction
The Communications Act (1934) (amended by the Telecommunications Act of 1996) (for common carriers)	Certain data privacy and security requirements for common carrier activities, such as television broadcasting, telephone, telegraph (but not radio), cable television, and broadband services	Federal Communications Commission
The Communications Act (1998) (for cable operators and satellite carriers)	Certain data privacy and security requirements for cable operators and satellite carriers	Federal Communications Commission
Video Privacy Protection Act (VPPA) (1988)	Certain requirements related to "personally identifiable information" for the purchase, renting, or delivery of videotapes or similar audiovisual materials	No agency specified
Family Educational Rights and Privacy Act (FERPA) (1974)	Certain requirements related to student education records maintained by educational institutions and institutions receiving federal funds	Department of Education
Federal securities laws	Certain requirements to protect information against data breaches and disclose data breaches for public companies and certain other companies	Securities and Exchange Commission
Children's Online Privacy Protection Act (COPPA) (1998)	Certain requirements for entities that collect and use children's information online	Federal Trade Commission
Electronic Communications Privacy Act (ECPA) (1986) [The Wiretap Act, the Stored Communications Act, and the Pen Register Act]	Rules for government entities and law enforcement related intercepting communication in transit or accessing stored information; certain provisions apply to private entities	No agency specified
Computer Fraud and Abuse Act (CFAA) (1986)	Rules related to the unauthorized access of "protected computers"(e.g., unauthorized intrusions or hacking)	No agency specified
Federal Trade Commission Act (1934)	Rules against "unfair" and "deceptive" data privacy and security practices; apply to most entities except common carriers, financial institutions, and nonprofits	Federal Trade Commission
Consumer Financial Protection Act (CFPA) (2010)	Rules against "unfair, deceptive, or abusive act or practice" in connection with "consumer financial product or service"[5]	Consumer Financial Protection Bureau (although it has been inactive in data privacy enforcement)

Source: Congressional Research Service[6]

[5] 12 U.S.C. § 5531(a).
[6] Mulligan, Stephen P., Freeman, Wilson C., and Linebaugh, Chris D. "Data Protection Law: An Overview." Congressional Research Service R45631, March 25, 2019. Retrieved from: https://sgp.fas.org/crs/misc/R45631.pdf.

At the same time, without a comprehensive federal privacy law, a growing number of states have sought to introduce privacy legislation, exacerbating the complexity of the U.S. privacy landscape. As of April 20, 2023, six states—California, Colorado, Connecticut, Iowa, Utah, and Virginia—have passed consumer data privacy laws (Table 2).[7] Despite some similarities, these privacy laws are characterized by differences in terms of entities and business activities subject to their jurisdiction, consumer rights, and business obligations. As of April 2023, at least twenty other states have introduced privacy legislation that are currently active, according to the International Association of Privacy Professionals (IAPP). [8]

The increasingly complex regulatory landscape poses a growing challenge for the private sector, which needs to comply with the rapidly evolving, divergent patchwork of federal and state privacy rules. As more states seek to pass new privacy laws, the U.S. digital single market risks suffering from growing regulatory fragmentation. In the absence of a federal privacy law with preemption powers, such a development could increase transaction costs, create new barriers to trade, and weaken awareness of consumer rights across state boundaries.[9]

It is against this backdrop that Florida lawmakers seek to pass yet another state privacy law.[10] Even if Florida's proposed legislation were better designed than the privacy laws of comparable states, it would nevertheless contribute to the growing risk of regulatory fragmentation. Such a development would come at a time when the Federal Trade Commission (FTC) seeks to pursue an increasingly activist approach to privacy issues based on an overly broad interpretation of its statutory authority under the FTC Act, representing yet another thicket of regulatory uncertainty in the U.S. data privacy landscape.

Table 2. U.S. State Data Privacy Laws

Legislation	Year
California Consumer Privacy Act (CCPA)	2018, effective Jan. 1, 2020
California Privacy Rights Act (CPRA)	2020; effective Jan. 1, 2023
Colorado Privacy Act (CPA)	2020; effective Jan. 1, 2023
Connecticut Data Privacy Act (CDPA)	2022, effective July 1, 2023
Iowa Consumer Data Protection Act (ICDPA)[11]	2023 (signed into law Mar. 28, 2023)
Virginia Consumer Data Protection Act (VCDPA)	2021; effective Jan. 1, 2023
Utah Consumer Privacy Act (UCPA)	2022, effective Dec. 31, 2023

Source: International Association of Data Privacy Professionals; Iowa State Legislature[12]

Overly Narrow Scope of Florida's Proposed Law Limits its Potential to Improve State-wide Privacy Practices

In the absence of a national data privacy framework, Florida lawmakers understandably seek to follow in the footsteps of several U.S. states and introduce state privacy legislation. However, to the extent Florida lawmakers seek to pass privacy legislation, Florida should establish a uniform set of consumer

[7] Additionally, a number of states, such as Illinois and Washington, have passed state-level biometric laws, which regulate how private entities collect and process biometric information. For a list of such laws, see "2023 State Biometric Privacy Law Tracker: A Comprehensive Resource for Tracking U.S. State Biometric Privacy Legislation." Husch Blackwell, Last updated April 10, 2023. Retrieved from: https://www.huschblackwell.com/2023-state-biometric-privacy-law-tracker.
[8] "US State Privacy Legislation Tracker: Consumer Privacy Bills." International Association of Privacy Professionals (IAPP), Last updated March 10, 2023. Retrieved from: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[9] McQuinn, Alan, and Castro, Daniel. "The Case for a U.S. Digital Single Market and Why Federal Preemption Is Key." Information Technology and Innovation Foundation, October 2019. Retrieved from: https://www2.itif.org/2019-dsm-preemption.pdf.
[10] H.B. 1547. S.B. 262.
[11] Since this policy brief was originally drafted before the signing into law of the Iowa Consumer Data Protection Act, the ICDPA has been excluded from the analysis of existing state-level privacy laws.
[12] "State Legislation Tracker." IAPP, Updated March 31, 2023. Retrieved from: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/. "Bill History for Senate File 262 - Status: Signed by Governor." Iowa Legislature, April 9, 2023. Retrieved from: https://www.legis.iowa.gov/legislation/billTracking/billHistory?billName=SF%20262&ga=90.

rights and business obligations based on whether and how companies use different types of sensitive personal data while taking steps to avoid imposing cumbersome regulations. In other words, privacy law should be industry neutral and create identical rules for firms in different sectors based on the risk of their data-related commercial activities, while creating some exemptions for startups and smaller companies (for example, exempting entities from certain requirements if they processed the data of fewer than 25,000 residents).

Instead of taking a risk-based, industry-neutral approach, Florida's proposed privacy law appears to target companies in specific sectors, i.e., as digital advertising and the manufacturing of smart devices. Unlike in Virginia, Connecticut, or Colorado, processing personal data of Florida residents beyond a certain threshold would not *per se* form a basis for jurisdiction under the House or the Senate version of the Florida legislation. Instead, Florida's proposed law would only apply to businesses with revenue of more than $1 billion that either 1) manufacture smart devices or 2) receive at least 50 percent of annual revenue from selling online- or targeted advertisement.[13]

However, consumer rights and business obligations are important not only for firms engaged in targeted sectors like digital advertising and smart device manufacturing, but potentially also for any entity processing or selling the sensitive personal data of a large number of consumers. Accordingly, states like Virginia and Connecticut have pursued a more general, risk-focused approach to data governance. For example, unlike Florida's proposed privacy law, Virginia's Consumer Data Protection Act does not set a minimum revenue threshold to fall under the scope of the law, nor does it target specific sectors. Instead, entities that conduct business or offer products or services "targeted" to Virginia residents could fall under the law's jurisdiction in two ways: 1) if they "control or process personal data of at least 100,000 consumers" or 2) if they "control or process personal data of at least 25,000 consumers *and* derive over 50 percent of gross revenue from the sale of personal data" (emphasis added).[14] As a result, companies can fall under the Virginia privacy law's jurisdiction if they control or process the sensitive personal data of over 100,000 consumers—irrespective of whether these entities sell advertisements or manufacture smart devices, unlike the case under Florida's proposed law.

Like Virginia, Connecticut's privacy statute follows a similar approach, although it adopts a lower revenue percentage threshold for jurisdiction. A firm would fall under the law's scope if it controls or processes personal data of 1) at least 100,000 Connecticut consumers or 2) of at least 25,000 consumers *and* derives more than 25 percent of its gross annual revenue from the sale of personal data.[15]

In contrast, companies that process or sell the sensitive data of Florida consumers, but fall below the revenue threshold or meet the other criteria, would remain beyond the scope of Florida's proposed law. In other words, the legislation's consumer rights and business obligations would not apply to the processing or sale of personal data unless these companies meet the narrowly defined criteria for jurisdiction. As a result, the potential of Florida's proposed privacy law to improve consumer rights and state-wide data practices across different sectors is limited.

Proposed Privacy Rules in the Florida Legislation Do Not Apply to Government Entities

Like the case under comparable state privacy laws, the Florida legislation's consumer rights and business obligation provisions would not apply in the context of data privacy practices of government and public sector entities. However, the growing number of data breaches at all levels of the U.S. government does not inspire confidence that federal agencies and state governments have a better track record than the private sector of protecting sensitive data.[16] As such, an ideal privacy law should also apply to government entities—which fall within the remit of the respective federal or state legislation—dealing with the personal data covered under the proposed law.

[13] H.B. 1547 § 501.173 (2) (e). S.B. 262 § 501.173 (2) (e).
[14] Code of Virginia § 59.1-576 (1).
[15] Connecticut General Statutes § 22-15 (2).
[16] Nabil, Ryan. "Biden Admin Must Engage Private Sector on Cybersecurity." *RealClearPolicy*, January 27, 2021. Retrieved from: https://www.realclearpolicy.com/2021/01/27/biden_admin_must_engage_private_sector_on_cybersecurity_657966.html.

Analyzing the European approach to data governance could be instructive in this regard. Notwithstanding some significant shortcomings, the European Union's General Data Protection Regulation (GDPR) applies to both private and public sector entities dealing with personal data (with some exceptions in emergency situations and on national security grounds).[17] That means that U.S. public sector entities are expected to comply with certain GDPR requirements when processing certain types of data of European data subjects—even though such actors might be exempt from most U.S. state and federal privacy rules. [18] By holding public entities to the same level of data privacy and security standards as the private sector, Florida can advocate a better approach to data privacy in the United States.

Consumer Rights and Business Obligations under Florida's Proposed Privacy Law

State privacy laws usually create a set of comparable consumer rights and business obligations in the context of data privacy and security practices. A nuanced understanding of consumer rights and business obligations in different state laws can help Florida lawmakers craft well-calibrated privacy rules that better balance the competing needs of data privacy, commercial needs, and technological innovation. In comparing existing state privacy statutes, the IAPP provides a useful definition of nine consumer rights and five business obligations that are commonly found in different U.S. data privacy laws (Tables A1 and A2).

Typical consumer rights in U.S. state privacy laws include, among others, a consumer's right to request data collected about the user, the right to request the correction of certain inaccurate data, and the right to request the deletion of data under certain conditions (Table A3). Likewise, common business obligations include requirements for businesses to provide notice about certain data practices and privacy policies, as well as restrictions on the collection and processing of personal information except for pre-specified purposes (Table A3).

While a detailed evaluation of Florida's legislative proposals falls beyond the scope of this policy brief, comparing Florida's proposed law to other state laws across common rights and obligations can enable a more well-informed understanding of the Florida privacy legislation (Tables A4 and A5). Although its narrow scope would limit the circumstances in which Florida consumers would enjoy the proposed consumer rights, these provisions are broadly comparable to consumer rights granted under Connecticut, Colorado, and Virginia's privacy laws (Table A4). For instance, Florida's proposed law would provide consumers with certain rights to access information that a data controller has collected about them (Table A4). Likewise, Florida's privacy legislation proposes the right to opt out of the sale of personal information and the right to request the correction and deletion of certain data (Table A4). However, unlike privacy laws in Colorado, Connecticut, and Virginia, Florida's privacy proposals do not include the right to opt out of processing for targeted advertisements and certain automated decision-making processes on websites (Table A4).

Most U.S. state privacy statutes do not provide a private right of action, apart from California, where two consumer privacy laws provide this right for certain violations, (Table A4). Unlike a different piece of privacy legislation introduced in Florida last year, the newly proposed law does not propose a right of private action, which would risk creating a litany of frivolous lawsuits. It is worth noting that the European Union—where civil law jurisdictions like France, Italy, and Spain do not share the highly litigious legal culture in the U.S.—only grants a rather limited right of private action under the GDPR.[19]

Apart from consumer rights, the Florida privacy legislation also proposes certain obligations for businesses, such as the duty to provide consumers with a notice about certain data practices and privacy policies (Table A5). It would also create an opt-in default for users under 18, meaning that

[17] EU Regulation 2016/679, Article 4 (7).

[18] Best, Best & Krieger LLP. "Public Agencies And GDPR Compliance - Government Entities Should Evaluate Data Collection And Use Practices." *JD Supra*, August 14, 2018. Retrieved from: https://www.jdsupra.com/legalnews/public-agencies-and-gdpr-compliance-24422/. "What Will ADPPA Compliance Entail?" *The HIPAA Journal*, July 7, 2022. Retrieved from: https://www.hipaajournal.com/adppa-compliance/.

[19] More specifically, under Article 80 (1) of the GDPR, data subjects can mandate a non-profit body, organization, or public-interest association to lodge a complaint on behalf of the data subject, while Article 82 (1) creates the right to compensation in case of damage due to infringement of GDPR rules.

businesses would need to gain express consent of users aged 13 to 18 and parental consent for users below 13 for the collection, processing, and sale of children's personal data (Table A5). However, unlike privacy laws in California, Colorado, and Connecticut, the Florida legislation does not propose creating a formal obligation on businesses to conduct risk assessments of privacy procedures and introduce restrictions on the collection and processing of personal information except for pre-specified purposes (Table A5). The Florida legislation also proposes certain obligations for social media platforms and search engines, which are discussed in later sections.

In summary, barring measures related to social media and search engines, the consumer rights and business obligation provisions of the Florida legislation are comparable to those in other U.S. privacy laws. However, the proposed consumer rights would not generally apply statewide to all Florida consumers generally, nor would business obligations apply to most Florida businesses. Instead, Florida residents would only enjoy the proposed consumer rights in the context of privacy practices of companies with annual revenue of over $1 billion that either manufacture smart devices or derive at least 50 percent of revenue from online or targeted advertisement.[20] In other words, while consumer rights provisions of the proposed Florida privacy law are comparable to those in other state privacy laws, consumers would enjoy these rights only in limited, specific circumstances where the business entity fulfills the comparatively narrow criteria for jurisdiction.

Proposed Transparency Rules for Social Media Platforms

The proposal in Florida has several unusual business obligations for social media platforms, which are uncharacteristic of any state-level consumer privacy laws in the United States. More specifically, the proposed law would bar government officers and salaried employees from using their position and state resources to communicate with social media platforms and request the removal of content or accounts.[21] It would also bar state and local government entities, officers, and employees from developing any agreements or working relationships with social media platforms for purposes of content moderation.[22]

While limiting government intervention in content moderation is a worthy goal, the extent to which such phenomena remain so commonplace as to merit legislation remains unclear. Also unclear is the extent to which such measures—even if they were needed—should be included in privacy law. Indeed, none of the existing U.S. state privacy laws or even the American Data Protection and Privacy Act introduced last year in Congress appear to include any such provisions. A better approach would entail passing separate legislation focused on creating privacy rules and delegating the question of social media regulation and rules for cooperation with government entities—if needed—to different legislation focused on such matters.

One positive aspect of the proposed Florida law is its efforts to implement better privacy protections for children. For example, the penalty for violations involving data subjects under 18 years can be up to three times as high as those for violations involving adult data subjects.[23] However, other social media proposals related to online safety raise several issues that need to be addressed. For instance, the House bill proposes to ban the use of "deceptive patterns, techniques, mechanisms or dark patterns to mislead or deceive children into making unintended or harmful decisions on the platform" without defining such terms.[24] What do "deceptive" or "dark patterns" or "unintended and harmful decisions" mean in the context of Florida's privacy legislation? The privacy laws of California and Connecticut—which stipulate that consumer consent must not be obtained using any "dark pattern"—adopt the FTC definition of "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation that consumer consent meant."[25]

[20] H.B. 1547 § 501.173 (2) (e). S.B. 262 § 501.173 (2) (e).
[21] Except in certain circumstances, e.g, law enforcement. H.B. 1547 § 112.23 (2). S.B. 262 § 112.23 (2).
[22] H.B. 1547 § 112.23 (3). S.B. 262 § 112.23 (3).
[23] H.B. 1547 § 112.23 (11) (a). S.B. 262 § 112.23 (11) (a).
[24] H.B. 1547 § 112.23 (10) (a).
[25] California Civil Code § 1798.140 (l). Connecticut General Statutes § 22-15 (11).

It is possible that Florida lawmakers might adopt the FTC definition of such terms, but that would still leave broader, more important questions. While efforts to investigate and address online safety issues are laudable, the extent to which they are best addressed through consumer privacy legislation, as opposed to separate online safety legislation, remains unclear. Also unclear is the question of whether and to what extent online safety rules in a rapidly evolving digital environment are best legislated at the federal or state level or developed by regulatory agencies with Congressional approval in response to emerging technologies and online safety challenges. At the very least, such terms as "deceptive practice" and "dark pattern" need to be debated, clarified, and defined more precisely if Florida lawmakers were to move forward with the proposed law.

Algorithmic Transparency for Search Engine Prioritization of "Political Partisanship" and " Ideology": A Step in the Wrong Direction

Unlike other state privacy laws in the United States, the two Florida bills also propose transparency requirements for search engines for political content in addition to privacy obligations. Both versions of the proposed law stipulate that "[a] controller that operates a search engine shall provide a consumer with information of how the controller's search engine algorithm prioritizes or deprioritizes political partisanship or political ideology in its search results."[26]

The choice of language— "how" search engines prioritize "political partisanship" and "ideology" as opposed to "whether" they do so— presupposes that search engines prioritize content as a function of political affiliation and ideology. As private entities, search engines should be free to prioritize or de-prioritize "politically partisan" or "ideological" content, but empirical evidence does not appear to support assertions that they do. In a December 2019 study, researchers at Stanford's Media Lab and School of Engineering found no evidence of political bias in their audit of search results for every candidate for federal office during the six months leading up to the 2018 U.S. elections.[27] Likewise, a statistical study conducted by *The Economist* in June 2019 found no evidence of ideological bias in Google search results, concluding that its search engine algorithms rewarded reputable reporting over, or rather than, left- or right-leaning news sources.[28]

To the extent that there is user-specific bias in search engine results, such biases often reflect a specific user's search history, browsing patterns, and preferences. As a general example, users that often visit French- or Spanish news sites would be more likely to be shown advertisements in those languages, compared to users who visit only English-language websites. Such mechanisms are typically designed to allow users to see content that she or he might find more interesting, relevant, or useful. In any event, such user-specific biases can be largely avoided by a combination of opting for privacy-oriented browsers, browsing in incognito mode, and utilizing a virtual private network.

Another potential reason for user-specific biases, as some computer scientists note, is that partisan differences in search terms can lead to divergent search engine results. Even then, according to a recent study, Google search engine results have been shown to demonstrate a mainstreaming effect that partially neutralizes the effects of partisan differences in search terms—instead of augmenting those differences as would be the case with algorithms that seek to prioritize partisan content.[29]

Furthermore, mandating the transparency of search engine algorithms reflects a certain misunderstanding of how search engine algorithms are different from social media content moderation practices. For example, in Facebook's determination of harmful content, content that

[26] H.B. 1547 § 112.23 (3) (b). S.B. 262 §112.23 (3) (b).
[27] Metaxa, Danaë, et al. "Search Media and Elections: A Longitudinal Investigation of Political Search Results." *Proceedings of the ACM on Human-Computer Interaction*, Volume 3, Issue CSCW, Article No. 129 (November 2019): 1–17. Retrieved from: https://doi.org/10.1145/3359231.
[28] "Google rewards reputable reporting, not left-wing politics." *The Economist*, June 8, 2019. Retrieved from: https://www.economist.com/graphic-detail/2019/06/08/google-rewards-reputable-reporting-not-left-wing-politics.
[29] Trielli, Daniel, and Diakopoulos, Nicholas. "Partisan search behavior and Google results in the 2018 U.S. midterm elections." *Information Communication & Society*, Volume 25, Issue 1 (May 18, 2020): 145–161. https://doi.org/10.1080/1369118X.2020.1764605.

is suspected of violating community standards or spreading "misinformation" is either reported by a user or flagged by an AI algorithm. The post is then reviewed by human content moderators (in case of suspected violations of community standards) or by fact-checkers (in case of suspected misinformation), who then make a determination on the content in question.[30] Unlike such multistep content moderation processes that could last days in cases involving human reviews, search engine results are instantaneous. Search engine results also require significantly complex calculations that keep changing and cannot always be explained clearly. That is especially the case with the rapid development of general-purpose AI systems and the application of AI algorithms to search engines, such as Microsoft Bing, Google Bard, and Webchat GPT.[31]

In developing AI systems, programmers often face a tradeoff between the "explainability" or transparency of AI algorithms and their underlying effectiveness. For example, medical researchers at New York's Mount Sinai Hospital developed an AI system—which trained on the medical data of 700,000 patients across several hundred variables—which could accurately provide medical diagnostics.[32] However, because of the complexity of algorithms, its programmers could not accurately describe how the algorithm functioned. If lawmakers were to mandate the explainability of algorithms, it could very well detract from the effectiveness of those systems.[33] At a time when a new generation of AI-enabled search engines are developing rapidly, mandating the explainability of search engine algorithms risks harming the quality and relevance of search results. If required at the federal level, such a policy could decelerate U.S. technological progress in developing the next generation of AI-enabled search engines—to the benefit of their global competitors.

Conclusion

Although Florida's proposed privacy law has certain positive features, its shortcomings far outweigh potential benefits. Consequently, if Florida lawmakers were to move ahead with the legislation, it would benefit from major revisions. At the very least, Florida's data privacy framework would benefit from a more evidence-based approach that considers the risks associated with different types and treatment of sensitive data—instead of an entity-focused approach that limits its jurisdiction to a handful of technology companies, search engines, and social media platforms. Creating privacy rules based on whether and how different entities use, process, and store different categories of sensitive data while minimizing regulatory burden could help improve statewide privacy practices, protect consumer rights, and create a more favorable regulatory environment.

However, even with an improved version, Florida's privacy legislation will be insufficient to deal with the regulatory complexities of an increasingly fragmented U.S. data privacy landscape. As more states pass privacy laws, more and more Florida businesses will need to comply with divergent privacy obligations and incur growing compliance costs—all the while dealing with growing regulatory activism from federal agencies. Without a national privacy framework that applies to all U.S.-domiciled entities, Florida lawmakers will also find it challenging to address regulatory loopholes that enable privacy violations of state residents by companies beyond its jurisdiction.

---

[30] The decision by a human content moderator or fact checker could potentially be appealed. See Barrett, Paul M. "Who Moderates the Social Media Giants? A Call to End Outsourcing." NYU Stern Center for Business and Human Rights, June 2020. Retrieved from: https://bhr.stern.nyu.edu/tech-content-moderation-june-2020.

[31] Shakir, Umar. "Bing, Bard, and ChatGPT: AI chatbots are rewriting the internet." *The Verge*, March 16, 2023. Retrieved from: https://www.theverge.com/23610427/chatbots-chatgpt-new-bing-google-bard-conversational-ai.

[32] Nabil, Ryan. "Strategies to Improve the National Artificial Intelligence Research and Development Strategic Plan." Competitive Enterprise Institute OnPoint No. 282, September 8, 2022. Retrieved from: https://cei.org/studies/strategies-to-improve-the-national-artificial-intelligence-research-and-development-strategic-plan/. Knight, Will. "The Dark Secret at the Heart of AI." *MIT Technology Review*, April 11, 2017. Retrieved from: https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/.

[33] Heaven, Will Douglas. "Why asking an AI to explain itself can make things worse." *MIT Technology Review*, January 20, 2020. Retrieved from: https://www.technologyreview.com/2020/01/29/304857/why-asking-an-ai-to-explain-itself-can-make-things-worse/.

It is in this context that Florida could play an important national role. As previously mentioned, current and proposed U.S. data privacy legislation do not typically apply to data practices of the U.S. government, federal agencies, and state and local governments. Florida lawmakers could champion the idea that the same privacy and cybersecurity standards should apply to U.S. government agencies and the private sector for dealing with similar types of data with comparable levels of associated risk. Lawmakers in Florida could also propose other tools—such as creating a federal regulatory sandbox for privacy—that could help create more flexible privacy rules for the changing needs of a growing U.S. digital economy.[34] By focusing legislative efforts on a federal level, Florida's leaders could play a much-needed national role in advocating rules that could improve nationwide data privacy practices, reduce barriers to digital trade, and promote the global competitiveness of the U.S. digital economy.

About the Author

Ryan Nabil is the Director of Technology Policy and Senior Fellow at the National Taxpayers Union Foundation.

[34] For a longer discussion on regulatory sandbox programs, Nabil, Ryan. "How Regulatory Sandbox Programs Can Promote Technological Innovation and Consumer Welfare: Insights from Federal and State Experience." Competitive Enterprise Institute OnPoint, August 17, 2022. Retrieved from: https://cei.org/wp-content/uploads/2022/08/Ryan_Nabil_-_Regulatory_Sandboxes-3.pdf.

Appendix

Table A1. Definitions of Common Consumer Rights under U.S. State Privacy Legislation	
Term	**Definition**
Right to access	The right for a consumer to access from a business/data controller the information or categories of information collected about a consumer, the information or categories of information shared with third parties, or the specific third parties or categories of third parties to which the information was shared; or, some combination of similar information.
Right to correct	The right for a consumer to request that incorrect or outdated personal information be corrected but not deleted.
Right to delete	The right for a consumer to request the deletion of personal information about the consumer under certain conditions.
Right to opt out of certain processing	The right of a consumer to restrict a business's ability to process personal information about the consumer.
Right to portability	The right for a consumer to request that personal information about the consumer be disclosed in a common file format.
Right to opt-out of sales	The right for a consumer to opt out of the sale of personal information about the consumer to third parties.
Right to opt-in for sensitive data processing	The right for a consumer to opt-in before a business can process their sensitive data.
Right against automated decision-making	A prohibition against a business making decisions about a consumer based solely on an automated process without human input.
Private right of action	The right for a consumer to seek civil damages from a business for violations of a statute.

Source: IAPP State Privacy Legislation Tracker[35]

Table A2. Definitions of Common Business Obligations under U.S. State Privacy Legislation	
Term	**Definition**
Opt-in default (requirement age)	A restriction placed on a business to treat consumers under a certain age with an opt-in default for the sale of their personal information.
Notice/transparency requirement	An obligation placed on a business to provide notice to consumers about certain data practices, privacy operations, and/or privacy programs.
Risk assessments	An obligation placed on a business to conduct formal risk assessments of privacy and/or security projects or procedures.
Prohibition on discrimination (exercising rights)	A prohibition against a business treating a consumer who exercises a consumer right differently than a consumer who does not exercise a right.
Purpose/processing limitation	An EU General Data Protection Regulation–style restrictive structure that prohibits the collection/processing of personal information except for a specific purpose.

Source: IAPP State Privacy Legislation Tracker

[35] "US State Privacy Legislation Tracker: Consumer Privacy Bills." IAPP, Last updated March 10, 2023. Retrieved from: https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf.

Table A3. Overview of Consumer Rights and Obligations under Florida's Proposed Privacy Legislation		
Consumer Rights		
Proposed consumer rights	**H.B. 1547**	**S.B. 162**
Right to access	Yes	Yes
Right to correct	Yes	Yes
Right to delete	Yes	Yes
Right to opt out of certain processing		
Right to portability	Yes	Yes
Right to opt out of sales	Yes	Yes
Right to opt-in for sensitive data protection		
Right against automated decision-making		
Private right of action		
Business Obligations		
Proposed business obligations	**H.B. 1547**	**S.B. 162**
Opt-in default (age requirement)	18 years	18 years
Notice/risk assessments	Yes	Yes
Prohibition on discrimination (exercising rights)		
Purpose/processing limitation		
Search engine disclosure requirement for prioritization of "political partisanship or political ideology"[36]*	Yes	Yes
Restrictions on "deceptive" practices on social media platforms*	Yes	Yes

Source: Author, Florida House Bill 1547, Florida Senate Bill 162

* Table A2, which is derived from IAPP, does not provide a definition for these two terms since these two business obligations are not characteristic of comparable state or federal privacy laws.

[36] More specifically, "[a] controller that operates a search engine shall provide a consumer with information of how the controller's search engine algorithm prioritizes or deprioritizes political partisanship or political ideology in its search results" [H.B. 1547 § 112.23 (3) (b), S.B. 262 § 112.23 (3) (b)].

Table A4. Comparing Consumer Rights under U.S. State Privacy Legislation[37]										
State	**Legislation**	**Right to access**	**Right to correct**	**Right to delete**	**Right to opt out of certain processing**	**Right to portability**	**Right to opt out of sales**	**Right to opt-in for sensitive data protection**	**Right against automated decision-making**	**Private right of action**
California	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	Yes		Yes		Yes	Yes			Private right of action limited to certain violations only.
California	California Privacy Rights Act (2020; effective Jan. 1, 2023)	Yes	Yes	Yes	Right to opt-out for sensitive data.	Yes	Yes		Yes	Private right of action limited to certain violations only.
Colorado	Colorado Privacy Act (2020; effective Jan. 1, 2023)	Yes	Yes	Yes	Right to opt-out of processing for profiling/ targeted advertising purposes.	Yes	Yes	Yes	Right to opt out of certain automated decision-making.	
Connecticut	Connecticut Data Privacy Act (2022; effective July 1, 2023)	Yes	Yes	Yes	Right to opt-out of processing for profiling/ targeted advertising purposes.	Yes	Yes	Yes	Right to opt out of certain automated decision making.	
Virginia	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	Yee	Yes	Yes	Right to opt-out of processing for profiling/ targeted advertising purposes.	Yes	Yes	Yes	Right to opt out of certain automated decision-making.	
Utah	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	Yes		Yes	Right to opt-out of processing for profiling/ targeted advertising purposes.	Yes	Yes			
Florida	House Bill 1547	Yes	Yes	Yes		Yes	Yes			
Florida	Senate Bill 262	Yes	Yes	Yes		Yes	Yes			

Source: IAPP State Privacy Legislation Tracker, H.B. 1547, S.B.162

[37] The appendix tables exclude the Iowa Consumer Data Protection Act, which was signed into law on March 28, 2023.

Table A5. Comparing Business Obligations under U.S. State Privacy Legislation								
State	Legislation	"Opt-in default (required age)"	"Notice/ transparency requirements"	Risk assessments	Prohibition on discrimination (exercising rights)	"Purpose/ processing limitation"	Notice for search engine prioritization of political content	Prohibition on "deceptive" practices on social media
California	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	16	Yes			Yes		
California	California Privacy Rights Act (2020; effective Jan. 1, 2023)	16	Yes	Yes	Yes	Yes		
Colorado	Colorado Privacy Act (2020; effective Jan. 1, 2023)	Sensitive Data, 13 years	Yes	Yes	Yes	Yes		
Connecticut	Connecticut Data Privacy Act (2022; effective July 1, 2023)	Sensitive Data, 13 years	Yes	Yes	Yes	Yes		
Virginia	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	Sensitive Data, 13 years	Yes	Yes	Yes	Yes		
Utah	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	13	Yes		Yes			
Florida	House Bill 1547	18[38]	Yes				Yes	Yes
Florida	Senate Bill 262	18[39]	Yes				Yes	Yes

Source: IAPP State Privacy Legislation Tracker, H.B. 1547, S.B.162.

[38] "A controller may not sell or share the personal information of a minor consumer if the controller has actual knowledge that the consumer is not 18 years of age or older. However, if a consumer who is between 13 and 18 years of age, or if the parent or guardian of a consumer who is 12 years of age or younger, has affirmatively authorized the sale or sharing of such consumer's personal information, then a controller may sell or share such information in accordance with this section." However, the proposed civil penalties can be tripled (from a base fine of up to $50,000 per violation) for any violation involving consumers 18 years of age or younger. H.B. 1547 § 112.23 (6) (b). S.B. 262 § 112.23 (6) (b).

[39] See above.

NATIONAL TAXPAYERS UNION

2023 National Taxpayers Union
122 C Street NW, Suite 700, Washington, DC 20001
ntu@ntu.org