The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Rules

BILL:	CS/CS/SB 262
INTRODUCER:	Rules Committee; Commerce and Tourism Committee; and Senator Bradley
SUBJECT:	Technology Transparency
DATE:	April 25, 2023 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	McMillan	McKay	CM	**Fav/CS**
2.	McMillan	Twogood	RC	**Fav/CS**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/SB 262 prohibits employees of a governmental entity from using their position or any state resources to communicate with a social media platform to request that it remove content or accounts. Additionally, a governmental entity cannot initiate or maintain any agreements with a social media platform for the purpose of content moderation. The bill provides certain exceptions.

The bill creates a unified scheme to allow Florida's consumers to control the digital flow of their personal data. Specifically, it gives consumers the right to:

- Confirm and access their personal data;
- Delete, correct, or obtain a copy of that personal data;
- Opt out of the processing of personal data for the 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;
- Opt out of the collection of sensitive data; and
- Opt out of the collection of personal data collected through the operation of a voice recognition feature.

The data privacy provisions of the bill generally apply to businesses that collect Florida consumers' personal data, make in excess of $1 billion in global gross annual revenues, and meet one of the following thresholds:

- Derives 50 percent or more if its global gross annual revenues from the sale of advertisements, including from providing targeted advertising or the sale of ads online;

- Operates 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
- Operates an app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

The bill requires a controller who operates an online search engine to make available an up-to-date plain language description of the main parameters that are most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results.

The Florida Department of Legal Affairs has authority to enforce the bill.

The bill also adds "biometric data" and "geolocation information" to the definition of "personal information" under the Florida Information Protection Act. As such, entities that possess fingerprints, DNA, and other biological or physiological identifying information must take reasonable measures to protect that data and report data breaches.

The bill takes effect on July 1, 2023.

II. Present Situation:

Internet and Social Media Platforms

There are many ways in which individuals access computer systems and interact with systems and other individuals on the Internet. Examples include:

- Social media sites, which are websites and applications, that allow users to communicate informally with others, find people, and share similar interests;[1]
- Internet platforms, which are servers used by an Internet provider to support Internet access by their customers;[2]
- Internet search engines, which are computer software used to search data (such as text or a database) for specified information;[3] and
- Access software providers, which are providers of software (including client or server software) or enabling tools for content processing.[4]

Such platforms earn revenue through various modes and models. Examples include:

[1] DelValle Institute Learning Center, *Social Media Platforms*, *available at* https://delvalle.bphc.org/mod/wiki/view.php?pageid=65 (last visited April 25, 2023).
[2] IGI Global, *Internet Platform*, *available at* https://www.igi-global.com/dictionary/internet-platform/15441 (last visited April 25, 2023).
[3] Merriam Webster, *Search Engine*, *available at* https://www.merriam-webster.com/dictionary/search%20engine (last visited April 25, 2023).
[4] 47 U.S.C. § 230(f)(4) defining "access software provider to mean a provider of software (including client or server software), or enabling tools that do any one or more of the following: (i) filter, screen, allow, or disallow content; (ii) pick, choose, analyze, or digest content; or (iii) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

- Data monetization.[5] This uses data that is gathered and stored on the millions of users that spend time on free content sites, including specific user location, browsing habits, buying behavior, and unique interests. This data can be used to help e-commerce companies tailor their marketing campaigns to a specific set of online consumers. Platforms that use this model are typically free for users to use.[6]
- Subscription or membership fees. This model requires users pay for a particular or unlimited use of the platform infrastructure.[7]
- Transaction fees. This model allows platforms to benefit from every transaction that is enabled between two or more actors. An example is AirBnB, where users transacting on the site are charged a fee.[8]

Freedom of Speech and Internet Platforms

Section 230

The federal Communications Decency Act (CDA) was passed in 1996 "to protect children from sexually explicit Internet content."[9] 47 U.S. Code § 230 (Section 230) was added as an amendment to the CDA to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum."[10]

Congress stated in Section 230 that "[i]t is the policy of the United States—(1) to promote the continued development of the Internet and other interactive computer services and other interactive media; [and] (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[11]

Specifically, Section 230 states that no provider or user of an interactive computer service may be held liable on account of:[12]

- Any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
- Any action taken to enable or make available to information content providers or others the technical means to restrict access to material from any person or entity that is responsible for

[5] The Alexander von Humboldt Institute for Internet and Society, *How do digital platforms make their money?*, July 29, 2019, *available at* https://www.hiig.de/en/how-do-digital-platforms-make-their-money/ (last visited April 25, 2023).
[6] Investopedia, *How Do Internet Companies Profit with Free Services?, available at* https://www.investopedia.com/ask/answers/040215/how-do-internet-companies-profit-if-they-give-away-their-services-free.asp#:~:text=Profit%20Through%20Advertising,content%20is%20through%20advertising%20revenue.&text=Each%20of%20these%20users%20represents,and%20services%20via%20the%20Internet (last visited April 25, 2023).
[7] HIIS, *supra* note 5.
[8] *Id.*
[9] *Force v. Facebook, Inc.*, 934 F.3d 53, 63 (2d Cir. 2019) (citing *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 173 (2d Cir. 2016) (citing 141 Cong. Rec. S1953 (daily ed. Feb. 1, 1995) (statement of Sen. Exon))).
[10] *Force*, 934 F.3d at 63 (quoting *Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 28 (2d Cir. 2015) (quoting *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997)).
[11] 47 U.S.C. § 230(b)(1)–(2).
[12] 47 U.S.C. § 230(c).

the creation or development of information provided through any interactive computer service.

Section 230 "assuaged Congressional concern regarding the outcome of two inconsistent judicial decisions,[13] both of which "appl[ied] traditional defamation law to internet providers."[14] The first decision held that an interactive computer service provider could not be liable for a third party's defamatory statement ... but the second imposed liability where a service provider filtered content in an effort to block obscene material."[15] To provide clarity, Section 230 provides that "[n]o provider ... of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.[16] In light of Congress's objectives, the Circuits are in general agreement that the text of Section 230(c)(1) should be construed broadly in favor of immunity.[17]

Section 230 specifically addresses how the federal law affects other laws. Section 230 prohibits all inconsistent causes of action and prohibits liability imposed under any State or local law.[18] Section 230 does not affect federal criminal law, intellectual property law, the Electronic Communications Privacy Act of 1986, or sex trafficking law.

There have been criticisms of the broad immunity provisions or liability shields which force individuals unhappy with third-party content to sue the user who posted it. While this immunity has fostered the free flow of ideas on the Internet, critics have argued that Section 230 shields publishers from liability for allowing harmful content.[19] Congressional and executive proposals to limit immunity for claims relating to platforms purposefully hosting content from those engaging in child exploitation, terrorism, and cyber-stalking have been introduced.[20] Bills have been filed that would require internet platforms to have clear content moderation policies, submit detailed transparency reports, and remove immunity for platforms that engage in certain behavioral advertising practices.[21] Proposals have also been offered to limit the liability shield for internet providers who restrict speech based on political viewpoints.[22]

Recently, the Supreme Court heard oral arguments in *Gonzalez v. Google LLC*, to determine whether online platforms should be held accountable when their algorithms prioritize or

[13] *Cubby, Inc. v. CompuServe, Inc*., 776 F. Supp. 135 (S.D.N.Y. 1991) and *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).
[14] *Force*, 934 F.3d at 63 (quoting *LeadClick*, 838 F.3d at 173).
[15] *Force*, 934 F.3d at 63 (quoting *LeadClick*, 838 F.3d at 173 (citing 141 Cong. Rec. H8469-70 (daily ed. Aug. 4, 1995) (statement of Rep. Cox))).
[16] 47 U.S.C. § 230(c)(1).
[17] *Force*, 934 F.3d at 63 (quoting *LeadClick*, 838 F.3d at 173).
[18] 47 U.S.C. § 230(e).
[19] Zoe Bedell and John Major, *What's Next for Section 230? A Roundup of Proposals* Lawfare, (July 29, 2020) https://www.lawfareblog.com/whats-next-section-230-roundup-proposals (last visited Feb. 25, 2021).
[20] *Id*; United States Department of Justice, Department of Justice's Review of Section 230 of the Communications Decency Act of 1996, https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996 (last visited Feb. 25, 2021); EARN IT Act of 2020, S.3398, 116th Cong. (2020).
[21] Bedell, s*upra* note 27; PACT Act, S.4066, 116th Cong. (2020); BAD ADS Act, S.4337, 116th Cong. (2020).
[22] Bedell, s*upra* note 27; Limiting Section 230 Immunity to Good Samaritans Act, S.3983, 116th Cong. (2020)

recommend certain content to its users.[23] The plaintiff in the case argues that Google aided and abetted international terrorism because its computer algorithms suggest certain content to its users based on their viewing history.[24] The district court granted Google's motion to dismiss based on Section 230, and the U.S. Court of Appeals for the Ninth Circuit affirmed.[25]

Search Engines

Search engines work by crawling billions of webpages, indexing the webpages, and then providing them to the person typing a query into the search engine.[26] A web crawler, also known as a bot, is a program that systematically browses the web to copy pages that are then processed by a search engine.[27] Next, the pages are indexed for easy retrieval.[28]

Each search engine uses their own algorithm, which determines the order pages appear.[29] Some choose to put emphasis on things like user experience, while others focus on content quality or link building.[30] Then a series of equations are used to determine where each piece of content should rank.[31]

Trade Secrets

Generally, trade secrets are intellectual property rights on confidential information that are used by a business and provide an economic advantage to that business.[32]

Section 812.081, F.S., defines a "trade secret" as information[33] used in the operation of a business, which provides the business an advantage or an opportunity to obtain an advantage, over those who do not know or use it. The test provided for in statute, and adopted by Florida courts,[34] requires that a trade secret be actively protected from loss or public availability to any person not selected by the secret's owner to have access thereto, and be:

- Secret;
- Of value;
- For use or in use by the business; and

---

[23] *See* Kaitlyn Tiffany, *The Supreme Court Considers the Algorithm* (Feb. 1, 2023) https://www.theatlantic.com/technology/archive/2023/02/supreme-court-section-230-twitter-google-algorithm/672915/ (last visited April 25, 2023).
[24] *See Gonzalez v. Google LLC*, 2 F.4th 871 (9th Cir. 2021).
[25] *Id*.
[26] *See* Anthony Schultes, *How Do Search Engines Work* (Sep. 9, 2021) *available at* https://www.seerinteractive.com/insights/how-do-search-engines-work (last visited April 25, 2023).
[27] *See* Cem Dilmegani, *Web Crawler: What it is, How it works & Applications in 2023* (March 6, 2023) *available at* https://research.aimultiple.com/web-crawler/ (last visited April 25, 2023).
[28] *Id*.
[29] *See* Anthony Schultes, *How Do Search Engines Work* (Sep. 9, 2021) https://www.seerinteractive.com/insights/how-do-search-engines-work (last visited April 25, 2023).
[30] *Id*.
[31] *Id*.
[32] *See* The Florida Bar, *Trade Secret* (Dec. 14, 2022) https://www.floridabar.org/practice-areas/trade-secrets/ (last visited April 25, 2023).
[33] A trade secret may manifest as any scientific, technical, or commercial information, including any design, process, procedure, list of suppliers, list of customers, business code, or improvement thereof. Section 812.081, F.S.
[34] See, e.g., *Sepro Corp. v. Dep't. of Envt'l. Prot.*, 839 So. 2d 781 (Fla. 1st DCA 2003).

- Of advantage to the business, or providing an opportunity to obtain an advantage, over those who do not know or use it. [35]

Penalties

Florida law criminalizes the disclosure or theft of trade secrets. For example:

- Section 815.04, F.S., makes it a third degree felony[36] for a person to willfully, knowingly, and without authorization disclose or take data, programs, or supporting documentation that are trade secrets that reside or exist internal or external to a computer, computer system, computer network, or electronic device.[37]
- Section 812.081, F.S., makes it a third degree felony for a person to steal, embezzle, or copy without authorization an article that represents a trade secret, when done with an intent to:
  - Deprive or withhold from the trade secret's owner the control of a trade secret, or
  - Appropriate a trade secret to his or her own use or to the use of another.

A number of statutes also provide non-criminal protections for trade secrets. The majority of these statutes provide public record exemptions for trade secrets,[38] but others provide procedural safeguards or civil remedies instead.[39]

Consumer Data Privacy Overview

Around 84 percent of Americans say they feel very little or no control over the data that is collected about them by both the government and private companies.[40] Business technology to collect and analyze data has grown, and companies regularly capture, store, and analyze data on their consumers.[41] While consumers often willingly agree to terms-of-service agreements to provide their data in exchange for free services, they are unaware of the extent to which that data is then used because the agreements are lengthy, overly-complicated, or simply not read by the consumer.[42]

---

[35] Section 812.081(1)(c), F.S.
[36] A third degree felony is punishable by up to 5 years imprisonment and a $5,000 fine. (ss. 775.082 and 775.083, F.S.)
[37] The offense is a second degree felony if committed for the purpose of creating or executing any scheme or artifice to defraud or to obtain property.
[38] Sections 119.071(1)(f), 125.0104(9)(d), 288.1226(8), 331.326, 365.174, 381.83, 403.7046(2)-(3), 403.73, 499.012(g), (m), 499.0121(7), 499.051(7), 499.931, 502.222, 570.48(3), 573.123(2), 581.199, 601.10(8)(a), 601.15(7)(d), 601.152(8)(c), 601.76, and 815.045, F.S.
[39] Sections 721.071 and 812.035, F.S.
[40] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, PEW RESEARCH CENTER, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over their Personal Information* at 7 (Nov. 15, 2019), *available at* https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf (last visited April 25, 2023).
[41] Max Freedman, BUSINESS NEWS DAILY, *How Businesses are Collecting Data (and What They're Doing With It)* (Jun. 17, 2020), *available at* https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (last visited April 25, 2023).
[42] Jessica Guynn, USA TODAY, *What Your Need to Know Before Clicking 'I Agree' on That Terms of Service Agreement or Privacy Policy* (Jan. 28, 2020),*available at* https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/ (last visited April 25, 2023).

Consumer data is most commonly tracked through the placement of 'cookies'—files that a website places in the user's device that allow for tracking across websites.[43] Another common tracker is a "fingerprinter," which creates a unique profile of the device, and allows the collector to gather information tied to that device.[44] These technologies allow websites to store a password that a consumer previously entered, and to follow the consumer's use patterns at other websites and to tailor their activities and advertisements to the consumer as a result of information it gleans.[45] Certain commercial businesses collect this information and create a consumer profile that describes possible interests or characteristics, and ultimately target ads for their products at the consumer.[46] Other companies—data brokers—collect and sell or share consumer data as their main business operation.[47]

Generally, the types of consumer data that businesses collect are:[48]

- Personal data, which includes personally identifiable information, such as Social Security numbers and gender, as well as identifiable information, including IP addresses, web browser cookies, and device IDs;
- Engagement data, which details how consumers interact with a business' website, mobile apps, social media pages, emails, paid ads, and customer service routes;
- Behavioral data, which includes transactional details such as purchase histories, product usage information, and qualitative data; and
- Attitudinal data, which encompasses metrics on consumer satisfaction, purchase criteria, product desirability, and more.

Federal and state governments have addressed data privacy and security to a certain extent, largely by targeting specific industries (e.g., healthcare and financial institutions) or types of data (such as children's personal information).[49] However, no federal law exists that comprehensively regulates how entities across all industries collect and use consumer data.[50] States have recently begun to legislate more comprehensively to protect data privacy.[51]

---

[43] NPR.org, *Online Trackers Follow our Digital Shadow by 'Fingerprinting' Browsers, Devices* (Sep. 26, 2016), *available at* https://www.npr.org/sections/alltechconsidered/2016/09/26/495502526/online-trackers-follow-our-digital-shadow-by-fingerprinting-browsers-devices (last visited April 25, 2023).

[44] *Id*.

[45] Wharton School of Business, University of Pennsylvania, *Your Data is Shared and Sold…What's Being Done About It?* (Oct. 28, 2019), *available at* https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ (last visited April 25, 2023).

[46] *See supra*, note 10

[47] Lois Beckett, PROPUBLICA, *Everything We Know About What Data Brokers Know About You* (June 13, 2014), *available at* https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you (last visited April 25, 2023). *See also* Louise Matsakis, Wired, *The WIRED Guide to Your Personal Data (and Who is Using It)*, (Feb. 15, 2019), *available at* https://www.wired.com/story/wired-guide-personal-data-collection/ (last visited April 25, 2023).

[48] Freedman, *supra*, note 10.

[49] Stephen Mulligan, Wilson Freeman, Chris Linebaugh, Congressional Research Service, *Data Protection Law: An Overview* at 7-8 (Mar. 25, 2019), *available at* https://crsreports.congress.gov/product/pdf/R/R45631 (last visited April 25, 2023).

[50] Wilson Freeman, Congressional Research Service, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress* (Nov. 1, 2018), *available at* https://crsreports.congress.gov/product/pdf/LSB/LSB10213/3 (last visited April 25, 2023).

[51] NCSL, *2021 Consumer Data Privacy Legislation* (Dec. 27, 2021),*available at* https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx (last visited April 25, 2023).

General Data Protection Regulation (GDPR)—European Union

The GDPR protects individual personal data and restricts entities' use of personal data, especially those that exercise overall control over the purpose and means of processing personal data (controllers) or that process data on behalf of, or at the instruction of controllers (processors).[52] A controller or processor is required to comply with the GDPR if it has activity in the European Union—even a minimal one, and regardless of where the data processing occurs.[53]

Personal data is defined as any information that relates to an identified or identifiable person, and can include names, identification numbers, location data, cookies, and any other information through which an individual can be directly or indirectly identified.[54] A processor and controller must receive express consent from an individual before they can collect or process his or her personal data. The language must give a clear choice that is not based on an overbroad or overly complex question.[55]

The GDPR requires entities subject to the GDPR to provide individuals with a report of their data that is processed, where it is processed, and why it is being processed.[56] This report must be provided to the individual within one month of his or her request.[57] If an individual makes a request that an entity correct or delete his or her personal data held by an entity, the entity must do so.[58]

State Data Privacy Regulations

California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

The CCPA (2018) defines personal information as that which identifies, relates to, describes, or is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household.[59] The CCPA grants consumers greater control over their personal information by, among other provisions, creating the following consumer rights, to:[60]

- Know about the personal information that a business collects, specifically about the consumer, and how it is used and shared;

---

[52] *See generally*, Stephen Mulligan, Wilson Freeman, Chris Linebaugh, CONGRESSIONAL RESEARCH SERVICE, *Data Protection Law: An Overview* p. 42 (Mar. 25, 2019), *available at* https://crsreports.congress.gov/product/pdf/R/R45631 (last visited April 25, 2023).
[53] GDPR, art. 3.
[54] GDPR, art. 4(1). *See*, U.K. Information Commissioner's Office, *Guide to General Data Protection Regulation: What is Personal Data? available at* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/ (last visited April 25, 2023).
[55] U.K. Information Commissioner's Office, *Guide to General Data Protection Regulation: Consent, available at* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (last visited April 25, 2023).
[56] Mark Kaelin, TECHREPUBLIC, *GDPR: A Cheat Sheet* (May 23, 2019), *available at* https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/ (last visited April 25, 2023).
[57] GDPR, arts. 12(3), 15.
[58] U.K. Information Commissioner's Office, *Guide to General Data Protection Regulation: Right to Erasure*, *available at* Right to erasure | ICO (last visited April 25, 2023).
[59] Cal. Civ. Code § 1798.140(v)(1).
[60] California Department of Justice, Office of the Attorney General, *California Consumer Privacy Act (CCPA)*, *available at* https://oag.ca.gov/privacy/ccpa (last visited April 25, 2023).

- Delete collected personal information with some exceptions;
- Opt out of the *sale* of personal information; and
- Be treated equally by covered businesses, whether or not an individual has exercised a right granted by the CCPA.

Additionally, the CCPA requires businesses to give consumers certain notices that explain their privacy practices and provide certain mechanisms to allow consumers to opt-out or exercise other rights regarding their personal information.

The CCPA applies to for-profit businesses that do business in California and that meet any of the following requirements:[61]

- Have a gross annual revenue of over $25 million;
- Buy, receive, or sell the personal information of 100,000 or more California residents, households, or devices; or
- Derive 50 percent or more of their annual revenue from selling California residents' personal information.

The law is largely enforced by the Attorney General, and businesses are subject to fines for violating the law. A consumer may only bring a cause of action against a business if certain categories of personal information tied to his or her name have been stolen in a nonencrypted and nonredacted form.[62]

The CPRA, which was approved by voters in a 2020 statewide ballot measure and took effect on January 1, 2023, amends and expands upon the CCPA.

The CPRA broadens consumers' rights by allowing them to:[63]

- Prevent businesses from *sharing* their personal information (CCPA prevents businesses from selling it);
- Correct their inaccurate personal information; and
- Limit a business' use of their sensitive personal information, which includes information such as a consumer's geolocation, race, ethnicity, religion, genetic data, private communications, sexual orientation, and specific health information.

The CPRA now applies to businesses that not only sell personal information, but also ones that share it. Additionally, the CPRA now prohibits sharing of data between different entities that make up a joint venture.[64]

[61] Cal. Civ. Code § 1798.140.
[62] Cal. Civ. Code ss. 1798.130, 1798.135.
[63] Elizabeth Shirley, *Overview of Applicability and Updated Privacy Provisions in the California Privacy Rights and Enforcement Act of 2020* (CPRA) (Jun. 10, 2021), *available at* https://www.jdsupra.com/legalnews/overview-of-applicability-and-updated-5551553/ (last visited April 25, 2023).
[64] *Id*.

The CPRA also provides that a business that collects personal information cannot retain a consumer's personal information or sensitive personal information for longer than is reasonably necessary.[65]

Virginia Consumer Data Protection Act

The Virginia Consumer Data Protection Act (Virginia Act) takes effect on January 1, 2023. The Virginia act grants consumers the right to access, correct, delete, obtain a copy of, and opt out of the processing of their personal data for the purposes of targeted advertising.[66] The Virginia Act defines "consumer" only as a natural person who is a resident of Virginia and acts only in an individual or household context.[67]

Businesses are subject to the Virginia Act if they operate in Virginia and either (1) control or process personal data of 100,000 or more consumers or (2) derive over 50 percent of their gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers.[68]

The Virginia Act exempts specific entities that are otherwise regulated by specific federal law, including those regulated by the GLBA and HIPAA. The Virginia Act also exempts Virginia public entities, nonprofit organizations, and higher education institutions.[69] In a similar vein, the Virginia Act exempts specific personal information, where the collection and use thereof is otherwise regulated by FCRA, FERPA, and COPPA.[70]

The Virginia Attorney General has exclusive authority to enforce the Virginia Act.[71]

Colorado Privacy Act

The Colorado Privacy Act (Colorado Act) will take effect on July 1, 2023.[72] Generally, with regard to personal data, the Colorado Act grants a consumer the right to:[73]

- Access data;

---

[65] Mario Meeks, JDSUPRA, *The CPRA's Storage Limitation Requirement is Coming—Practical Tips for Shoring Up Your Record Retention Practices to Comply* (Feb. 18, 2021), *available at* https://www.jdsupra.com/legalnews/the-cpra-s-storage-limitation-9898179/ (last visited April 25, 2023).

[66] Va. Code Ann. § 59.1-573 (2020). *See also*, Colleen Brown, Alan Raul, Lauren Kitces, Sidley LLP, *East Coast Meet West Coast: Enter the Virginia Consumer Data Privacy Protection Act* (Mar. 5, 2021), *available at* https://www.sidley.com/en/insights/newsupdates/2021/03/east-coast-meets-west-coast-enter-the-virginia-consumer-data-protection-act (last visited April 25, 2023).

[67] Va. Code Ann. § 59.1-571 (2020).

[68] Va. Code Ann. § 59.1-572 A (2020).

[69] Va. Code Ann. § 59.1-572 B (2020).

[70] Va. Code Ann. § 59.1-572 C (2020).

[71] *See generally*, Kurt Hunt and Matthew Diaz, JDSUPRA, *Virginia Becomes 2nd State to Adopt a Comprehensive Consumer Data Privacy Law* (Mar. 4, 2022), *available at* https://www.natlawreview.com/article/virginia-becomes-2nd-state-to-adopt-comprehensive-consumer-data-privacy-law (last visited April 25, 2023).

[72] C.R.S. 1-6-1301-1313, *available at* https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf (last visited April 25, 2023).

[73] The National Law Review, *And Now There are Three…The Colorado Privacy Act*, July 16, 2021, *available at* https://www.natlawreview.com/article/and-now-there-are-three-colorado-privacy-act#:~:text=Colorado%20has%20now%20joined%20California,effect%20on%20July%201%2C%202023. (last visited April 25, 2023).

- Correct data;
- Delete data;
- Data portability;
- Opt out of the sale of personal information, targeted advertising, and profiling;
- Appeal; and
- Non-discrimination.

Like the CCPA and Virginia Act, the Colorado Act contains exceptions for certain types of data and information governed by federal law. It provides that the Attorney General has exclusive authority to enforce violations of the law, and does not provide a private cause of action to a consumer. The Colorado Act applies to persons conducting business in the state that either:[74]

- Control or process personal data of 100,000 or more consumers during a calendar year; or
- Derive revenue or receive discounts from the sale of personal data and control or process data of at least 25,000 consumers.

The Colorado Act does not bestow a private right of action. The Colorado Attorney General has exclusive enforcement authority to prosecute violations as deceptive trade practices.[75]

Utah Consumer Privacy Act

The Utah Consumer Privacy Act (UCPA) will take effect on December 31, 2023.[76] Generally, with regard to personal data, the UCPA grants a consumer the right to:

- Access data;
- Delete data;
- Obtain a copy of data;
- Opt out of the sale of data; and
- Opt out of targeted advertising.[77]

Unlike the CCPA, the Colorado Act, and the Virginia Act, the UCPA does not provide consumers with the ability to correct personal data.[78] The UCPA applies to a controller or processor that conducts business in Utah or produces a product or service targeted to Utah residents, has annual revenues of $25,000,000 or more, and satisfies at least one of the following thresholds:

- During a calendar year, controls or processes the personal data of 100,000 or more Utah residents; or
- Derives over 50% of its gross revenue from the sale of personal data, and controls or processes the personal data of 25,000 or more consumers.[79]

[74] *Id.*
[75] Weiner Brodsky Kider, PC, *Colorado Enhances Data Privacy for Consumers* (Aug. 10, 2021), *available at* https://www.jdsupra.com/legalnews/colorado-enhances-data-privacy-for-7292123/ (last visited April 25, 2023).
[76] The National Law Review, *Utah Becomes Fourth U.S. State to Enact Consumer Privacy Law* (March 24, 2022), *available at* Utah Consumer Privacy Act Passed - UCPA Legislation (natlawreview.com) (last visited April 25, 2023).
[77] *Id.*
[78] *Id.*
[79] *Id.*

The UCPA does not provide a private right of action. The Utah Attorney General will enforce the law.[80]

***Florida Information Protection Act (FIPA)*[81]**

FIPA is a data security measure that requires governmental entities, specific business entities, and any third-party agent that holds or processes personal information on behalf of these entities to take reasonable measures to protect a consumer's personal information. Additionally, FIPA requires covered business entities[82] that are subject to data breaches to attempt to remediate the breach by notification to affected consumers in Florida, and in cases where more than 500 individual's information was breached—by additional notification to the Department of Legal Affairs (DLA).[83] If the breach affected more than 1,000 individuals in Florida, the entity must also notify credit reporting agencies, with certain exceptions.[84]

FIPA defines "personal information" as:

- Online account information, such as security questions and answers, email addresses, and passwords; and
- An individual's first name or first initial and last name, in combination with any one or more of the following information regarding him or her:
  - A social security number;
  - A driver license or similar identity verification number issued on a government document;
  - A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
  - Medical history information or health insurance identification numbers; or
  - An individual's health insurance identification numbers.[85]

Personal information does not include information:

- About an individual that a federal, state, or local governmental entity has made publicly available; or
- That is encrypted, secured, or modified to remove elements that personally identify an individual or that otherwise renders the information unusable.[86]

FIPA does not provide a private cause of action, but authorizes the DLA to file charges against covered entities under Florida's Unfair and Deceptive Trade Practices Act (FDUTPA).[87]

---

[80] *Id.*
[81] Section 501.171, F.S.; Chapter 2014-189, Laws of Fla. (FIPA expanded and updated Florida's data breach disclosure laws contained in s. 817.5681, F.S. (2013), which was adopted in 2005 and repealed in 2014).
[82] A "covered entity" is a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. Section 501.171(1)(b), F.S.
[83] Florida Office of the Attorney General (OAG), *How to Protect Yourself: Data Security*, *available at* http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C (last visited April 25, 2023). Section 501.171(3)-(4), F.S.
[84] Section 501.171(3)-(6), F.S.
[85] Section 501.171(1)(g)1., F.S.; OAG *supra* note 41.
[86] Section 501.171(1)(g)2., F.S.
[87] Section 501.171(9), (10), F.S.; OAG *supra* note 41.

In addition to the remedies provided for under FDUTPA, a covered entity that fails to notify DLA, or an individual whose personal information was accessed, of the data breach is liable for a civil penalty of $1,000 per day for the first 30 days of any violation; $50,000 for each subsequent 30-day period of violation; and up to $500,000 for any violation that continues more than 180 days. These civil penalties apply per breach, not per individual affected by the breach.

Illinois Biometric Information Privacy Act

In 2008, Illinois became the first state to specifically regulate biometric data with the passage of the Biometric Information Privacy Act (BIPA). BIPA puts in place safeguards and procedures that relate to the retention, collection, disclosure, and destruction of biometric information and specifically protects the biometric information of those in Illinois.

BIPA defines biometric data as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

Under BIPA, a private entity:[88]

- That possesses biometric data must have a written policy that establishes a retention schedule and guidelines for permanently destruction of such data;
- Cannot collect, capture, purchase, receive through trade, or otherwise obtain biometric data unless it receives an informed release from the subject;
- Cannot profit from a person's biometric data;
- Cannot disseminate a person's biometric data unless the subject consents or provides authorization, or the entity is required by law or a valid warrant or subpoena; and
- Must store, transmit, and protect biometric data with a reasonable standard of care and in a manner as or more protective as other confidential and sensitive information.

BIPA provides a private cause of action, with relief including liquidated damages, ranging from $1,000 to $5,000 or actual damages (whichever is greater), attorney's fees and costs, and other relief deemed appropriate by a court.[89]

The Illinois Supreme Court found that an individual does not need to allege an actual injury or adverse effect, beyond violation of their rights under BIPA, to qualify as an aggrieved party. Therefore, anyone whose biometric data is affected by a violation of BIPA may seek liquidated damages or injunctive relief under BIPA.[90] Court documents also tend to support the notion that an individual in Illinois has a valid cause of action if their biometric data is taken without consent by a private entity, including out-of-state entities, but it is subject to a finding of fact.[91]

[88] 740 Ill. Comp. Stat. 14/10, 14/15 (2008).
[89] 740 Ill. Comp. Stat. 14/20 (2008).
[90] *See Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.
[91] *See Rivera v. Google, Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017); *See also In re Facebook Biometric Information Privacy Litigation*, 185 F.Supp.3d 1155 (N.D. Cal. (2016).; *See also Norberg v. Shutterfly, Inc.*, 152 F.Supp.3d 1103 (N.D. Ill. 2015).

Federal Privacy Regulations

Health Insurance Portability and Accountability Act (HIPAA)[92] and its Related Rules

HIPPA requires federal agencies to create national standards to protect sensitive patient health information from disclosure without the patient's consent or knowledge. HIPPA's two pertinent implementing rules are the Privacy Rule and the Security Rule.[93]

The Privacy Rule addresses the use and disclosure of individual's protected health information (PHI) by covered entities.[94, 95] PHI is information, including demographic data, that can be used to identify the individual, and that relates to the individual's:

- Past, present, or future physical or mental health or physical condition;
- Health care; or
- Payment for past, present, or future health care.

A common example of PHI is a patient's name, address, birth date, or social security number. However, PHI does not include deidentified health information or employment-related records.

The Privacy Rule protects PHI that is held or transmitted by a covered entity or its business associate by preventing covered entities from disclosing PHI without the patient's consent or knowledge unless it is being used or shared for treatment, payment, or healthcare operations or for another exempt purpose.

These covered entities must prominently post an electronic notice and give notice upon a specific request to patients regarding the manners in which they use and disclose PHI. A covered entity must also provide an accounting of disclosures it has made of a patient's PHI upon his or her request as well as a copy of his or her PHI.

The Security Rule applies to the subset of identifiable health information that a covered entity creates, receives, maintains, or transmits in electronic form called "electronic protected health information" (e-PHI).[96] The Security Rule does not apply to PHI that is transmitted orally or in writing. A covered entity must comply with the Security Rule by:

- Ensuring the confidentiality, integrity, and availability of all e-PHI;
- Detecting and safeguarding against anticipated threats to the security of the information;
- Protecting against anticipated uses or disclosures; and
- Certifying compliance by their workforce.

---

[92] 42 U.S.C. § 1320.

[93] *See generally*, Stephen Mulligan, Wilson Freeman, Chris Linebaugh, Congressional Research Service, *Data Protection Law: An Overview* pp. 10-12 (Mar. 25, 2019), *available at* https://crsreports.congress.gov/product/pdf/R/R45631 (last visited April 25, 2023).

[94] 45 C.F.R. §160 and 164. *See also*, Department of Health and Human Services, *Summary of the HIPPA Privacy Rule*, (Jul. 26, 2013) *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited April 25, 2023).

[95] A covered entity is a health plan, health care clearinghouse, health care provider who transmits health information in electronic form, and these entities' business associates.

[96] 45 C.F.R. §164.302-318.

The Department of Health and Human Services may institute a civil enforcement under HIPPA and may seek civil penalties. The Department of Justice may institute criminal proceedings against a violator who knowingly obtained or disclosed PHI. There is no private cause of action under HIPPA.

Federal Policy for the Protection of Human Subjects ("Common Rule")

The Common Rule is promulgated by the U.S. Food and Drug Administration (FDA) and governs the ethical conduct of research involving human subjects.[97] Fifteen federal agencies and departments are party to this rule. The Common Rule mandates that researchers protect the privacy of subjects and maintain confidentiality of human subject data, among other requirements.[98]

The FDA is a member of the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, which brings together the regulatory authorities and the pharmaceutical industry to develop guidelines for pharmaceutical trials.[99]

Fair Credit Reporting Act (FCRA)[100]

The FCRA promotes the accuracy, fairness, and privacy of information that consumer reporting agencies and their related entities collect.[101] The FCRA governs the acts of credit reporting agencies (CRAs), entities that furnish information to CRAs (furnishers), and individuals who use credit reports issued by CRAs. Specifically, CRAs and their furnishers must adopt methods to ensure the information they collect and report is accurate.

Individuals can review the information a CRA has collected on them to ensure that it is accurate, and may dispute its accuracy—which triggers a CRA's and furnisher's duty to reinvestigate the information. Individuals may also request to review the information a CRA has in his or her file, the sources of the information, and the identity of those to whom the information was disclosed.

A CRA cannot provide information in a consumer report to anyone who does not have a specified purpose in the FCRA.[102]

The FTC and Consumer Finance Protection Bureau share civil enforcement authority of the FCRA. A person who willfully obtains consumer information from a CRA under false pretenses

---

[97] 21 C.F.R. §§ 50, 60.
[98] *See generally*, Health and Human Services, *Federal Policy for the Protection of Human Subjects ('Common Rule')* (Mar. 18, 2016), *available at* https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html (last visited April 25, 2023).
[99] International Council for Harmonisation, *available at* https://www.ich.org/ (last visited April 5, 2023).
[100] 15 U.S.C. §1681.
[101] Consumer Finance Bureau, *A Summary of Your Rights Under the Fair Credit Reporting Act* (Sept. 18, 2018), 12 CFR 1022, *available at* A Summary of Your Rights Under the Fair Credit Reporting Act (ftc.gov) (last visited April 25, 2023). *See also*, Federal Trade Commission, *Fair Credit Reporting Act*, *available at* https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited April 25, 2023).
[102] Permissible purposes include employment, insurance underwriting that involves the consumer, evaluating the consumer's eligibility for licensure or other governmental benefit that considers the applicants financial responsibility or status, or a legitimate business need. 15 U.S.C. § 1681b(a).

is subject to criminal prosecution. An individual may also pursue a private right of action if he or she was injured by willful or negligent actions.[103]

Gramm-Leach Bliley Act (GLBA)[104]

The GLBA governs financial institutions' use and protection of nonpublic personal information (NPI).[105] A financial institution is any institution that engages in financial activities, such as banks, real estate appraisers and title companies, consumer-financing companies, insurance underwriters and agents, wire transfer agencies, check cashing stores, and mortgage brokers.[106]

A financial institution cannot share (1) NPI with non-affiliated third parties unless they notify the consumer of their intent to do so and provide a chance to opt out; and (2) a consumer's account or credit card numbers with third parties for direct marketing. The financial institution must also send an annual notice to the consumer that clearly and conspicuously describes the institution's privacy policies and practices.[107]

The financial institution must also ensure the security and confidentiality of a customer's NPI by establishing concrete security policies, and by designating an information security program coordinator and implementing a risk assessment process.[108]

The Consumer Financial Protection Bureau, Federal Trade Commission, and federal banking agencies share civil enforcement authority of the GLBA. Certain civil remedies and criminal liabilities are available for violations of the data security and protection provisions of the GLBA, but there is no private cause of action.

Children's Online Privacy Protection Act (COPPA)[109]

COPPA and its related rules regulate websites' collection and use of children's information. The operator of a website or online service that is directed to children, or that has actual knowledge that it collects children's personal information (covered entities), must comply with requirements regarding data collection and use, privacy policy notifications, and data security.

COPPA defines personal information as individually identifiable information about an individual that is collected online, including:

---

[103] An individual may record actual damages, attorney's fees, litigation costs, and in the case of willful violations—statutory damages ranging from $100 to $1,000 and punitive costs as the court deems appropriate. 15 U.S.C. § 1681n(a).
[104] 15 U.S.C. §§ 6801-6809. *See generally*, Stephen Mulligan, Wilson Freeman, Chris Linebaugh, Congressional Research Service, *Data Protection Law: An Overview* pp. 8-10 (Mar. 25, 2019), *available at* https://crsreports.congress.gov/product/pdf/R/R45631 (last visited April 25, 2023).
[105] The GLBA defines "nonpublic personal information" as "personally identifiable information" that is not publicly available and is either provided by the consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by the financial institution. 15 U.S.C. § 6809(9).
[106] Federal Trade Commission, *FTC Safeguards Rule: What Your Business Needs to Know* (May, 2022) *available at* https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited April 25, 2023).
[107] The notice must specifically include the categories of NPI the financial institution collects and discloses, the types of third parties with which it shares NPI, and how it protects consumers' NPI.
[108] *See*, 16 C.F.R. § 314.4
[109] 16 C.F.R. pt. 312.

- A first and last name;
- A home or other physical address, e-mail address, telephone number, or any other identifier that the FCC determines could permit one to contact someone physically or online, such as a screen name;
- A social security number;
- A persistent identifier that can be used to recognize a user over time and across different websites;
- A photograph, video, or audio file that contains a child's image or voice;
- A geolocation information that is sufficient to identify the user's location; or
- Information concerning the child or parents that the operator collects from the child and combines with any other identifier described above.

A covered entity may not collect a child's (individual under the age of 13) personal information without the prior, verifiable consent of his or her parent.[110]

COPPA further requires covered entities to:[111]

- Give parents direct notice of their privacy policies, including a description of their data collection and sharing practices;
- Post a clear link to their privacy policies on their home page and at each area of their website where they collect personal information from children;
- Institute procedures to protect the personal information that they hold;
- Ensure that any third party with which they share collected personal information implements the same protection procedures; and
- Delete children's personal information after the purpose for its retention has been fulfilled.

Violations of COPPA are an unfair or deceptive act or practice and are prosecuted by the FTC. COPPA also authorizes state attorneys general to enforce violations that affect residents of their states. There is no criminal prosecution or private right of action provided for under COPPA.[112]

Driver's Privacy Protection Act (DPPA)[113]

The DPPA prohibits state Departments of Motor Vehicle (DMVs) from releasing an individual's personal information obtained by the DMV in connection with a motor vehicle record, subject to certain exceptions, such as a legitimate government need. Additionally, the DPPA requires DMVs to obtain an individual's consent to enable the sale or release of personal motor vehicle record to a third-party marketer.

---

[110] 15 U.S.C. §§ 6502(a)-(b).
[111] *See*, Federal Trade Commission, *General Questions About the COPPA Rule: What is the Children's Online Privacy Protection Rule?*(Jul. 2020), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (last visited April 25, 2023).
[112] Federal Trade Commission, *General Questions About the COPPA Rule: COPPA Enforcement*, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (last visited April 25, 2023).
[113] 18 U.S.C. §2721.

Violations of the DPPA are subject to criminal fine. Additionally, a private individual affected by the improper disclosure or use of his or her personal information may bring a private civil action against the violator.[114]

Family Educational Rights and Privacy Act (FERPA)[115]

FERPA protects the privacy of student's education records. The law applies to any school that receives applicable funds from the U.S. Department of Education. FERPA grants parents certain rights respecting their child's education records, and this privacy right transfers to the student when he or she reaches age 18 or attends a post-secondary school.

Schools may disclose, without consent, directory information, such as a student's name, address, telephone number, birthday, place of birth, honors and awards, and dates of attendance. However, schools must disclose and allow parents and students to opt out of the disclosure of their directory information.

Schools must give an annual notice about rights granted by FERPA to affected parties.[116]

Federal Trade Commission Act (FTC Act)

The FTC protects consumer data privacy by acting under Section 5 of the FTC Act, which bars unfair and deceptive acts and practices that affect commerce.[117] Specifically, the FTC prosecutes companies that act unfairly or deceptively when they gather, use, or disclose personal information in a manner that contradicts their posted privacy policy or other statements, or fail to implement reasonable data security safeguards.[118]

For example, the FTC prosecuted both Sears and Upromise for drafting misleading privacy policies that did not fully disclose the extent to which a consumer's online browsing would be tracked.[119]

---

[114] 18 U.S.C. § 2724. *See generally*, Electronic Privacy Information Center, *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*, *available at* The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record – EPIC – Electronic Privacy Information Center (last visited April 25, 2023).

[115] 20 U.S.C. §1232(g); 34 C.F.R. § 99.

[116] U.S. Department of Education, *Family Educational Rights and Privacy Act (FERPA)*, (Aug. 25, 2021) *available at* https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (last visited April 25, 2023).

[117] 15 U.S.C. § 1681. Federal Trade Commission, *Privacy and Security Enforcement*, *available at* https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited April 25, 2023).

[118] Stephen Mulligan, Wilson Freeman, Chris Linebaugh, CONGRESSIONAL RESEARCH SERVICE, *Data Protection Law: An Overview* p. 30-35 (Mar. 25, 2019), *available at* https://crsreports.congress.gov/product/pdf/R/R45631 (last visited April 25, 2023).

[119] *See, e.g.*, Federal Trade Commission, *Membership Reward Service Upromise Penalized for Violating FTC Order* (Mar. 17, 2017) Stephen Mulligan, Wilson Freeman, Chris Linebaugh, Congressional Research Service, *Data Protection Law: An Overview* p. 42 (Mar. 25, 2019), *available at* https://crsreports.congress.gov/product/pdf/R/R45631 (last visited April 25, 2023); and Complaint *In the Matter of Sears Holdings Mgmt Co.*, No. C-4264 (F.T.C. Aug. 31, 2009).

III. Effect of Proposed Changes:

Governmental Content Moderation of Social Media Platforms

Section 1 creates s. 112.23, F.S., to prohibit government directed content moderation of social media platforms. A social media platform is a form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content. A governmental entity is any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law.

The bill prohibits an officer or a salaried employee of a governmental entity from using their position or any state resources to communicate with a social media platform to request that it remove content or accounts from the social media platform. Additionally, a governmental entity, or an officer or a salaried employee acting on behalf of a governmental entity may not initiate or maintain any agreements or working relationships with a social media platform for the purpose of content moderation.

The bill provides that the above prohibitions to do not apply if the governmental entity or an officer or a salaried employee acting on behalf of a governmental entity is acting as part of any of the following:

- Routine account management of the government entity's account, including but not limited to the removal or revision of the governmental entity's content or account or identification of accounts falsely posing as a government entity or officer or salaried employee;
- An attempt to remove content that pertains to the commission of a crime or violation of Florida's public records law;
- An attempt to remove an account that pertains to the commission of a crime or violation of Florida's public records law; or
- An investigation or inquiry related to an effort to prevent imminent bodily harm, loss of life, or property damage.

Consumer Data Privacy

Sections 2 creates a new part V of ch. 501, F.S., entitled "Data Privacy and Security."

Section 3 creates s. 501.701, F.S., entitled the "Florida Digital Bill of Rights."

Definitions

Section 4 creates s. 501.702, to provide definitions used throughout the bill including the following:

- "Biometric data" means data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs, video or audio recordings or data generated from video or audio recordings, or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

- "Child" means an individual younger than 18 years of age.
- "Controller" means:
  - A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:
    - Is organized or operated for the profit or financial benefit of its shareholders or owners;
    - Conducts business in this state;
    - Collects personal data about consumers, or is the entity on behalf of which such information is collected;
    - Determines the purposes and means of processing personal data about consumers alone or jointly with others;
    - Makes in excess of $1 billion in global gross annual revenues; and
    - Satisfies at least one of the following:
      - Derives 50 percent or more of its global gross annual revenues from providing targeted advertising or the sale of ads online;
      - Operates 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. For purposes of this sub-subparagraph, a consumer smart speaker and voice command component service does not include a motor vehicle or speaker or device associated with or connected to a vehicle which is operated by a motor vehicle manufacturer or a subsidiary or affiliate thereof; or
      - Operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.
  - Any entity that controls or is controlled by a controller. The term "control" means:
    - Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller;
    - Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
    - The power to exercise a controlling influence over the management of a company.
- "Decision that produces a legal or similarly significant effect concerning a consumer" means a decision made by a controller which results in the provision or denial by the controller of any of the following:
  - Financial and lending services;
  - Housing, insurance, or health care services;
  - Education enrollment;
  - Employment opportunities;
  - Criminal justice; or
  - Access to basic necessities, such as food and water.
- "Personal data" means any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.
- "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, which directly identifies the specific location of an individual with precision and accuracy within a

radius of 1,750 feet. The term does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility.

- "Processor" means a person who processes personal data on behalf of a controller.
- "Search engine" means technology and systems that use algorithms to sift through and index vast third-party websites and content on the Internet in response to search queries entered by a user. The term does not include the license of search functionality for the purpose of enabling the licensee to operate a third-party search engine service in circumstances where the licensee does not have legal or operational control of the search algorithm, the index from which results are generated, or the ranking order in which the results are provided.
- "Sensitive data" means a category of personal data which includes any of the following:
  - Personal data revealing an individual's racial 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; and
  - Precise geolocation data.
- "Targeted advertising" means displaying to a consumer an advertisement selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests. The term does not include any of the following:
  - An advertisement that is:
    - Based on activities within a controller's own website or online application;
    - Based on the context of a consumer's current search query, visit to a website, or use of an online application; or
    - Directed to a consumer in response to the consumer's request for information or feedback; or
  - The processing of personal data solely for measuring or reporting advertising performance, reach, or frequency.
- "Voice recognition feature" means the function of a device which enables the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds.

Applicability

Section 5 creates s. 501.703, F.S., to provide that the consumer data privacy provisions apply to a person that conducts business in Florida or produces a product or service used by residents of Florida, and processes or engages in the sale of personal data. It does not apply to the processing of personal data by a person in the course of a purely personal or household activity. A controller or processor that complies with the Children's Online Privacy Protection Act is in compliance with requirements to obtain parental consent.

The consumer data privacy provisions do not apply to the following:

- A state agency;
- A financial institution or data subject to the federal Gramm-Leach-Bliley Act's privacy protections;
- A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services in

accordance with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the federal Health Information Technology for Economic and Clinical Health Act;
- A nonprofit organization; or
- A postsecondary education institution.

Exemptions

Section 6 creates s. 501.704, F.S., to provide that the following information is exempt from the consumer data privacy provisions:
- Protected health information under the Health Insurance Portability and Accountability Act of 1996.
- Health records.
- Patient identifying information for purposes of 42 U.S.C. s. 290dd-2.
- Identifiable private information:
  - For purposes of federal policy for protection of human subjects under 45 C.F.R. Part 46;
  - Collected as part of human subjects research under the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or of the protection of human subjects under 21 C.F.R. parts 50 and 56; or
  - That is personal data used or shared in research conducted in accordance with the requirements set forth in the bill or other research conducted in accordance with applicable law.
- Information and documents created for purposes of the Health Care Quality Improvement Act of 1986.
- Patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005.
- Information derived from any health care-related information listed under s. 501.704, F.S., that is deidentified in accordance with the requirements for deidentification under the Health Insurance Portability and Accountability Act of 1996.
- Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under s. 501.704, F.S., which is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996, or by a program or a qualified service organization as defined by 42 U.S.C. s. 290dd-2.
- Information that is included in a limited data set as described by 45 C.F.R. s. 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by 45 C.F.R. s. 164.514(e).
- Information used only for public health activities and purposes described in 45 C.F.R. s. 164.512.
- Information collected or used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act of 1996.
- The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, credit standing, and other factors by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act.

- Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994.
- Personal data regulated by the Family Educational Rights and Privacy Act of 1974.
- Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1971.
- Data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.
- Data processed or maintained as the emergency contact information of an individual under this part that is used for emergency contact purposes.
- Data that is processed or maintained and is necessary to retain to administer benefits for another individual that relates to an individual described as an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, and used for the purposes of administering those benefits.
- Personal data collected and transmitted which is necessary for the sole purpose of sharing such personal data with a financial service provider solely to facilitate short term, transactional payment processing for the purchase of products or services.
- Personal data collected, processed, sold, or disclosed in relation to price, route, or service as those terms are used in the Airline Deregulation Act, by entities subject to that act, to the extent the provisions of this bill is preempted by 49 U.S.C. s. 41713.
- Personal data shared between a manufacturer of a tangible product and authorized third-party distributors or vendors of the product, as long as such personal data is used solely for advertising, marketing, or servicing the product that is acquired directly through such manufacturer and such authorized third-party distributors or vendors. Such personal data may not be sold or shared unless otherwise authorized under this part.

Consumer Rights

Section 7 creates s. 501.705, F.S., to establish a set of rights for consumers with respect to their personal data. A consumer is entitled to exercise these rights at any time by submitting a request to a controller. The request must specify the applicable rights the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise the consumer rights on the child's behalf.

The bill requires a controller to comply with an authenticated consumer request to exercise any of the following rights:

- **To confirm** whether a controller is processing the consumer's personal data, and to access the personal data;
- **To correct inaccuracies** in the consumer's personal data, taking into account the nature of the data and the purposes of the processing of the data;
- **To delete personal data** provided by or obtained about the consumer;
- **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;
- **To opt out of the processing** of the 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.

- **To opt out of the collection of sensitive data**, including precise geolocation data, or the processing of such data; or
- **To opt out of the collection of personal data collected through the operation of a voice recognition feature.**

Controller Response to Consumer Request

Section 8 creates s. 501.706, F.S., to provide that a controller must respond to a consumer request without undue delay, which may not be later than 45 days after the date of receipt of the request, except that the controller may extend the response period once by an additional 15 days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension and the reason for the extension within the initial 45 day response period. If a controller cannot take action regarding the consumer's request, the controller must inform the consumer without undue delay, which may not be later than 45 days after the date of receipt of the request, of the justification for the inability to take action and must also provide instructions on how to appeal the decision.

The bill provides that a controller is not required to comply with a consumer request, if the controller cannot authenticate the request. However, the controller must make a reasonable effort to work with the consumer to authenticate the consumer and the consumer's request. If a controller maintains a self-service mechanism to allow a consumer to correct certain personal data, the controller may require the consumer to correct their own personal data through such mechanism. A controller must provide the consumer with notice within 60 days of the request that the controller has complied with the consumer's request.

The bill requires a controller to provide information in response to a request free of charge, at least twice annually per consumer, except that if a request is manifestly unfounded, excessive, or repetitive, the controller may charge a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request altogether. The controller bears the burden of demonstrating that the request is manifestly unfounded, excessive, or repetitive.

A controller that has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer's request to delete that personal data by taking either of the following actions:

- Deleting the personal data, retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records, and not using the retained data for any other purpose; or
- Opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt from regulations under the bill

Appeal

Section 9 creates s. 501.707, F.S., to require a controller to establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request. A controller must inform the consumer in writing of any action taken or not taken in response to an

appeal within 60 days after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

Waiver or Limitation of Consumer Rights

Section 10 creates s. 501.708, F.S., to provide that any provision of a contract or agreement which waives or limits in any way a consumer right established by the data privacy provisions in the bill is void and unenforceable as contrary to public policy.

Submitting Consumer Requests

Section 11 creates s. 501.709, F.S., to require a controller to establish two or more secure, reliable, and conspicuously accessible methods to enable consumers to submit a request to exercise their consumer rights. The methods must take all of the following into account:

- The ways in which consumers normally interact with the controller;
- The necessity for secure and reliable communications of the requests; and
- The ability of the controller to authenticate the identity of the consumer making the request.

A controller may not require a consumer to create a new account to exercise their rights, but a controller may require a consumer to use an existing account.

The bill requires a controller to provide a mechanism on its website for consumers to submit requests for information required to be disclosed. However, a controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal information may also provide an email address for the submission of requests for such information.

Controller Duties

Section 12 creates s. 501.71, F.S., to require a controller to limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that data is processed, as disclosed to the consumer. Additionally, a controller must establish, implement, and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue, for the purposes of protecting the confidentiality, integrity, and accessibility of personal data.

The bill prohibits a controller from doing any of the following:

- Processing personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purpose for which the data is processed, as disclosed to the consumer, without the consumer's consent, except as otherwise provided by the bill.
- Processing personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers.
- Discriminating against a consumer for exercising any of the consumer rights contained in the bill, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer. However, a controller may offer financial incentives, including payments to consumers as compensation, for 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. The consent may be revoked by the consumer at any time.
- Processing a consumer's sensitive data without obtaining the consumer's consent, or, in processing the sensitive data of a known child, without processing that data with the affirmative authorization for such processing of a known child who is between 13 and 18 years old in accordance with the federal Children's Online Privacy Protection Act.

The prohibition against discrimination based on a consumer's exercise of their consumer rights may not be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised their right to opt out of the processing of their personal data for purposes of targeted advertising, data sales, or profiling or if the offer is related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

The bill requires a controller who operates an online search engine to make available in an easily accessible location on the webpage that does not require a consumer to log in or register to read, an up-to-date plain language description of the main parameters that are most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. Algorithms are not required to be disclosed or any information that would enable deception or harm to consumers through the manipulation of search results.

Privacy Notices

Section 13 creates s. 501.711, F.S., to require a controller to provide consumers with a reasonably accessible and clear privacy notice, updated at least annually, that includes all of the following information:
- The categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller;
- The purpose of processing personal data;
- How consumers may exercise their rights, including the process that a consumer may use to appeal a controllers decision with regard to the consumer’s request;
- If applicable, the categories of personal data that the controller shares with third parties;
- If applicable, the categories of third parties with whom the controller shares personal data; and
- A description of the methods a consumer may use to exercise their consumer rights under the data privacy provisions of the bill.

The bill requires a controller that engages in the sale of personal data that is sensitive data to provide the following notice: “NOTICE: This website may sell your sensitive personal data.”

The bill requires a controller that engages in the sale of personal data that is biometric data to provide the following notice: “NOTICE: This website may sell your biometric personal data.”

A controller that sells personal data to third parties or processes personal data for targeted advertising must clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process. Additionally, a controller may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with the appropriate notice.

Duties of Processor

Section 14 creates s. 501.712, F.S., to require a controller to adhere to the instructions of a controller, and must assist the controller in meeting or complying with the controller's duties.

A processor must do the following:

- Assist the controller in responding to consumer rights requests, by using appropriate technical and organizational measures;
- Assist the controller in complying with the requirement relating to the security of processing personal data and to the notification of breach of security of the processor's system under s. 501.171, F.S., taking into account the nature of processing and the information available to the processor; and
- Provide necessary information to enable the controller to conduct and document data protection assessments.

The bill provides that a contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must include all of the following information:

- Clear instructions for processing data;
- The nature and purpose of processing;
- The type of data subject to processing;
- The duration of processing;
- The rights and obligations of both parties; and
- A requirement that the processor:
    - Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
    - At the controller's direction, delete or return all personal data to the controller as requested after the provisions of the service is completed, unless retention of the personal data is required by law;
    - Make available to the controller, upon reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with the data privacy provisions of the bill;
    - Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and
    - Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.

The bill authorizes a processor to arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the requirements under the data privacy provisions of the bill. Additionally, the processor must provide a report of the assessment to the controller upon request.

The bill prohibits the above provisions from being construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by the data privacy provisions of the bill. Additionally, the bill provides that a determination of whether a person is acting as a controller or processor with respect to a specific processing of data is a fact based determination that depends on the context in which personal data is to be processed and further establishes that a processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains in the role of a processor.

Data Protection Assessments

Section 15 creates s. 501.713, F.S., to require a controller to conduct and document a data protection assessment of each of the following processing activities involving personal data:

- The processing of personal data for purposes of targeted advertising;
- The sale of personal data;
- The processing of sensitive data;
- Any processing activities involving personal data that present a heightened risk of harm to consumers; and
- The processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:
  - Unfair or deceptive treatment of or unlawful disparate impact on consumers;
  - Financial, physical, or reputational injury to consumers;
  - A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or
  - Other substantial injury to consumers.

The bill requires a data protection assessment to do the following:

- Identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce such risks; and
- Factor the following into the assessment:
  - The use of deidentified data;
  - The reasonable expectations of consumers;
  - The context of the processing; and
  - The relationship between the controller and the consumer whose personal data will be processed.

The bill requires the controller to make an assessment available to the attorney general on request pursuant to a civil investigative demand. However, the disclosure of the assessment in compliance with a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

The bill provides that a single data protection assessment may address a comparable set of processing operations which include similar activities. Additionally, a data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may

constitute compliance with the bill's requirements if the assessment has a reasonably comparable scope and effect.

The bill provides that this section only applies to processing activities generated on or after July 1, 2023.

Deidentified Data, Pseudonymous Data, and Aggregate Consumer Information

Section 16 creates s. 501.714, F.S., to require a controller in possession of deidentified data to do the following:

- Take reasonable measures to ensure that the data cannot be associated with an individual;
- Maintain and use the data in deidentified form;[120]
- Contractually obligate any recipient of the deidentified data to comply with the data privacy provision of the bill; and
- Implement business processes to prevent inadvertent release of deidentified data.

The bill provides that a controller or processor may not be required to do the following:

- Reidentify deidentified data or pseudonymous data;
- Maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or
- Comply with an authenticated consumer rights request, if the controller:
  - Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to do so;
  - Does not use the personal data to recognize or respond to the specific consumer who is the subject of the data or associate the data with other personal data about the same specific consumer; and
  - Does not sell the personal data to any third party or otherwise voluntarily disclose the data to any third party other than a processor, except as otherwise permitted.

The bill provides that controller duties regarding transparency and consumer rights to confirm, access, correct, delete, and obtain a copy of their personal data are inapplicable to pseudonymous data or aggregate consumer data in cases in which the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

The bill requires a controller that discloses pseudonymous data, deidentified data, or aggregate consumer information to exercise reasonable oversight to monitor compliance with any contractual commitments to which the data or information is subject. Additionally, a controller must take appropriate steps to address any breach of those contractual commitments.

[120] The bill provides that a controller may not attempt to reidentify the data, except that the controller may attempt to reidentify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of s. 501.714, F.S.

Requirements for Sensitive Data

Section 17 creates s. 501.715, F.S., to provide that a person who meets s. 501.702 (9)(a)1., (a)2., and (a)3., for the definition of a controller may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer, or if the sensitive data is of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in accordance with the Children's Online Privacy Protection Act. Additionally, a person who engages in the sale of personal data that is sensitive data must provide the following notice: "NOTICE: This website may sell your sensitive personal data." A person who violates this provision is subject to enforcement under the data privacy provisions of the bill.

Exemptions for Certain Uses of Consumer Personal Data

Section 18 creates s. 501.716, F.S., to provide that a controller or processor may not be restricted from the following:

- Complying with federal or state laws, rules or regulations;
- Complying with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
- Investigating, establishing, exercising, preparing for, or defending legal claims;
- Providing a product or service that is specifically requested by a consumer or, if applicable, their parent or guardian;
- Taking immediate steps to protect an interest that is essential for life or physical safety and in which the processing cannot be manifestly based on another legal basis;
- Preventing, detecting, protecting against, or responding to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;
- Preserving the integrity or security of systems or investigating, reporting, or prosecuting those responsible for breaches of system security;
- Assisting another controller, processor, or third party in complying with the requirements in the bill;
- Disclosing personal data disclosed when a consumer uses or directs the controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party;[121]
- Transferring personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that the information is used or shared consistently with the requirements in this bill;[122] or
- Engaging in public or peer-reviewed scientific or statistical research in the public interest which adheres to all other applicable ethics and privacy laws and is approved, monitored, and

[121] The bill provides that an intentional interaction occurs when the consumer intends to interact with the third party, by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

[122] The bill provides that if a third party materially alters how it uses or shares the personal data of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it must provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that consumers can easily exercise choices consistent with the bill.

governed by an institutional review board or similar independent oversight entity that determines:
- Whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;
- Whether the expected benefits of the research outweigh the privacy risks; and
- Whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

The bill provides that a controller or processor is not prevented from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Florida law as part of a privileged communication. Additionally, the bill may not be construed as imposing a requirement on controllers and processors that adversely affects the rights or freedoms of any person, including the right of free speech; or require a controller, processor, third party, or consumer to disclose a trade secret.

Collection, Use, or Retention of Data for Certain Purposes

Section 19 creates s. 501.717, F.S., provide that the requirements imposed on controllers and processors under the bill may not restrict a controller's or processor's ability to collect, use, or retain data to do any of the following:
- Conducting internal research to develop, improve, or repair products, services, or technology;
- Effecting a product recall;
- Identifying and repairing technical errors that impair existing or intended functionality; or
- Performing certain internal operations that are:
  - Reasonably aligned with the expectations of the consumer;
  - Reasonably anticipated based on the consumer's existing relationship with the controller; or
  - Otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

The bill requires that a requirement imposed on a controller or processor under the bill is inapplicable if compliance would violate an evidentiary privilege under Florida law.

Disclosure of Personal Data to Third-party Controller or Processor

Section 20 creates s. 501.718, F.S., to establish that a controller or processor that discloses personal data to a third-party controller or processor who is in violation of the consumer data privacy provisions of the bill is not also themselves in violation if the disclosure was done in compliance with the bill and, at the time of the disclosure, the disclosing controller or processor could not have reasonable known that the recipient intended to commit a violation. Additionally, a third-party controller or processor that receives personal data from a controller or processor who is in compliance with the data privacy provisions of the bill is not considered in violation of the bill for the violations of the controller or processor from which the third-party controller or processor receives the personal data.

Processing of Certain Personal Data by Controller or Other Person

Section 21 creates s. 501.719, F.S., to provide that personal data processed by a controller pursuant to ss. 501.716, 501.717, and 501.718 may not be processed for any purpose other than a purpose listed in ss. 501.716, 501.717, and 501.718. Personal data processed by a controller in ss. 501.716, 501.717, and 501.718, may be processed to the extent that the processing of the data is:

- Reasonably necessary and proportionate to the purposes listed in ss. 501.716, 501.717, and 501.718;
- Adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in ss. 501.716, 501.717, and 501.718; and
- Done to assist another controller, processor, or third party with any of the purposes specified in ss. 501.716, 501.717, and 501.718.

The bill provides that personal data collected, used, or retained under s. 501.717, F.S., must take into account the nature and purpose of such collection, use, or retention. Such personal data is subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

The bill provides that a controller that processes personal data under an exemption under s. 501.719, F.S., bears the burden of demonstrating that the processing of the personal data qualifies for the exemption and complies with all requirements.

The bill requires a controller or processor to adopt and implement a retention schedule that prohibits the use or retention of personal data not subject to an exemption by the controller or processor after the satisfaction of the initial purpose for which the information was collected or obtained, after the expiration or termination of the contract pursuant to which the information was collected or obtained, or 2 years after the consumer's last interaction with the controller or processor. This requirement does not apply to the following:

- To provide a good or service requested by the consumer, or reasonably anticipate the request of such good or service within the context of a controller's ongoing business relationship with the consumer;
- To debug to identify and repair errors that impair existing intended functionality; or
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller or that are compatible with the context in which the consumer provided the information.

Agency Enforcement and Implementation

Section 22 creates s. 501.72, F.S., to provide that the Department of Legal Affairs (DLA) may prosecute on behalf of a Florida consumer any violation of the bill's data privacy provisions as a deceptive and unfair trade practice, pursuant to the Florida Deceptive and Unfair Trade Practices Act (FDUTPA).[123]

[123] For the purpose of brining an action pursuant to this bill ss. 501.211 and 501.212, F.S., do not apply.

The DLA may provide suspected controller, processor, or third party violators a right to cure their violation by providing written notice of the violation and then allowing a 45-day period to cure the alleged violation. However, the DLA cannot offer a right to cure based on an alleged violation that involves a Florida consumer who the controller, processor, or third party has actual knowledge is under 18 years old. If the alleged violator cures the violation to the satisfaction of the DLA, the DLA may issue a letter of guidance. If the violator fails to cure within 45 days, the DLA may commence enforcement against the controller, processor, or third party.

The court may:
- Grant injunctive relief;[124]
- Award actual damages based on the violation;[125]
- Award a civil penalty of not more than $50,000 for each willful violation; and
- Triple the civil penalty if the violation:
  - Involves a Florida consumer who the controller, processor, or third party knows is 18 years of age or younger;
  - Is based on a controller's, processor's, or third party's failure to delete or correct the consumer's personal information after receiving an authenticated request to delete or correct, unless otherwise exempt; or
  - Is based on the controller's, processor's, or third party's continued sale or sharing of the consumer's personal information after the consumer opted out.

The bill grants the DLA rulemaking authority to implement the bill, including the adoption of standards for authenticated consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf. The DLA may employ or use the legal services of outside counsel and the investigative services of outside personnel. Additionally, the DLA may collaborate and cooperate with other enforcement authorities of the federal government or other state governments if such enforcement authorities have restrictions governing confidentiality that are at least as stringent as the restrictions in this bill.

Liability for a tort, contract claim, or consumer protection claim that is unrelated to an action brought under the bill does not arise solely from the failure of a controller, processor, or third party to comply with this bill.

The bill provides that there is not a private cause of action.

Report by the Department of Legal Affairs

The bill requires the DLA to make a report publicly available by February 1 each year on the DLA's website that describes any actions it has undertaken to enforce the bill. The report must include statistics and relevant information that details:
- The number of complaints received and the categories or types of violations alleged by the complainant;
- The number and type of enforcement actions taken and the outcomes of such action;
- The number of complaints resolved without the need for litigation; and

[124] Section 501.207(1), F.S.
[125] Section 501.207(1), F.S.

- For the report due February 1, 2024, the status of the development and implementation of rules to implement the bill.

The bill provides that for purposes of bringing an action, any person who meets the definition of controller as defined in the bill who collects, shares, or sells the personal data of Florida consumers is considered to be engaged in both substantial and not isolated activities within Florida and operating, conducting, engaging in, or carrying on a business, and doing business in Florida, and thus, subject to the jurisdiction of the courts of Florida.

Preemption

Section 23 creates s. 501.721, F.S., to provide that consumer data privacy is a matter of statewide concern and the bill supersedes all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection, processing, sharing, or sale of consumer personal information by a controller or processor. The regulation of the collection, processing, sharing, or sale of consumer personal information by a controller or processor is preempted to the state.

Florida Information Protection Act (FIPA)

Section 24 amends s. 501.171, F.S., to include an individual's biometric data and any information regarding an individual's geolocation in FIPA's definition of "personal information" so that covered entities are required to notify the affected individual, the DLA, and credit reporting agencies of a breach of biometric information or geolocation paired with an individual's first name or first initial and last name.

Legal Affairs Revolving Trust Fund

Section 25 amends s. 16.53, F.S., to require all money recovered by the Attorney General for attorney fees, costs, and penalties in an action for a violation of this bill must be deposited in the Legal Affairs Revolving Trust fund.

Effective Date

The bill takes effect on July 1, 2023.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None Identified.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

This will likely have wide-ranging impact on how Florida consumers interact with websites and internet-connected devices.

Businesses will have to adjust their operations to implement the bill's notice and privacy requirements. Many of the businesses subject to the bill's requirements may have already implemented or are in the process of implementing similar privacy practices based on legislation in other states, and the E.U.

Search engines will have to provide information to consumers on how the search engine prioritizes or deprioritizes certain information.

C. Government Sector Impact:

Governmental entities may have to update their policies to reflect the prohibitions in the bill.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

The bill substantially amends the following sections of the Florida Statutes: 16.53 and 501.171.

This bill creates the following sections of the Florida Statutes: 112.23, 501.701, 501.702, 501.703, 501.704, 501.705, 501.706, 501.701, 501.708, 501.709, 501.71, 501.711, 501.712, 501.713, 501.714, 501.715, 501.716, 501.717, 501.718, 501.719, 501.72, and 501.721.

IX. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS/CS by Rules on April 24, 2023:
The committee substitute does the following:

- Clarifies that the prohibition against government directed content moderation of social media platforms does not pertain to an investigation/inquiry related to an effort to prevent imminent bodily harm, loss of life, or property damage.
- Provides that the consumer data provisions apply to a person that does business in Florida or produces a product or service used by Florida residents, and processes or engages in the sale of personal data.
- Provides that a consumer has a right to do the following:
  - Confirm whether a controller is processing the consumer's personal data, and can access the personal data;
  - Correct inaccuracies in the consumer's personal data, taking into account the nature of the data and the purposes of the processing of the data; and
  - Delete personal data provided by or obtained about the consumer;
- 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;
- Opt out of 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;
- Opt out of the collection of sensitive data, including precise geolocation data, or the processing of such data; or
- Opt out of the collection of personal data collected through the operation of a voice recognition feature.
- Requires a controller to respond to a consumer request no later than 45 days after the request is made. The controller can extend the response period once by an additional 15 days if reasonably necessary. However, a controller is not required to comply with a consumer request, if the controller cannot authenticate the request.
- Requires a controller to establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision.
- Requires a controller to establish two or more secure, reliable, and conspicuously accessible methods to enable consumers to submit a request to exercise their consumer rights and sets out certain factors those methods must take into account.
- Provides that operating an app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install, is one of the factors that makes a business fall under the definition of controller, if they meet the other threshold criteria provided in the definition.
- Provides exemptions for the use of certain data, and provides that certain restrictions on the collection and retention of data for particular purposes is prohibited.
- Requires a controller to limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which that data is processed, as disclosed to the consumer. Additionally, a controller that operates an

online search engine must make available an up-to-date plain language description of the main parameters, including the relative importance of those main parameters that are most significant in determining ranking in search results.

- Provides that a processor, defined as a person that processes data on behalf of the controller, is required to adhere to instructions given by the controller and assist the controller in complying with the bill.
- Requires a controller to conduct and document a data protection assessment, which is required to weigh the benefits of the processing activity against the potential risks to the rights of the consumer, including any safeguards that could mitigate risk.
- Requires a controller in procession of deidentified data to take steps to ensure that the data cannot be associated with an individual.
- Prohibits a person who meets specific criteria from engaging in the sale of personal data that is sensitive data without prior consent of the consumer.
- Adds definitions of "search engine" and "dark pattern."

CS by Commerce and Tourism on April 4, 2023: The committee substitute clarifies that the prohibitions provided in section 1 of the bill do not apply to a governmental entity that is acting as part of any of the following:

- An attempt to remove content that pertains to the commission of a crime or violation of Florida's public records law; or
- An attempt to remove an account that pertains to the commission of a crime or violation of Florida's public records law.

B. Amendments:

None.