**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 Commerce and Tourism

| | |
|---|---|
| BILL: | SB 262 |
| INTRODUCER: | Senator Bradley |
| SUBJECT: | Technology Transparency |
| DATE: | April 3, 2023 |
| REVISED: | |

| | ANALYST | STAFF DIRECTOR | REFERENCE | ACTION |
|---|---|---|---|---|
| 1. | McMillan | McKay | CM | **Pre-meeting** |
| 2. | | | JU | |
| 3. | | | RC | |

## I. Summary:


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 government 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 information. Specifically, it gives consumers the right to:

- Access their personal information;
- Delete or correct that personal information; and
- Opt out of the sale or sharing of their personal information.

The Act generally applies to businesses that collect Florida consumers' personal information, make in excess of $1 billion in gross revenues, and meet one of the following thresholds:

- Derives 50 percent or more if its global annual revenues from providing targeted advertising or the sale of ads online; or
- Operated 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.

The bill prohibits the collection of a consumer's precise geolocation data or personal information through the operation of a voice recognition feature, unless the consumer provides authorization.

The bill requires a search engine to provide a consumer with information on how the search engine algorithm prioritizes or deprioritizes political partisanship or political ideology in its search results.

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

The bill also adds "biometric data," "genetic information," and "geolocation data" 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 January 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:

- 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]

---

[1] DelValle Institute Learning Center, *Social Media Platforms*, *available at* https://delvalle.bphc.org/mod/wiki/view.php?pageid=65 (last visited April 3, 2023).
[2] IGI Global, *Internet Platform*, *available at* https://www.igi-global.com/dictionary/internet-platform/15441 (last visited April 3, 2023).
[3] Merriam Webster, *Search Engine*, *available at* https://www.merriam-webster.com/dictionary/search%20engine (last visited April 3, 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.
[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 3, 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 3, 2023).
[7] HIIS, *supra* note 5.

- 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]

**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.[9] 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.[10] Next, the pages are indexed for easy retrieval.[11]

**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.[12] Business technology to collect and analyze data has grown, and companies regularly capture, store, and analyze data on their consumers.[13] 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.[14]

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.[15] 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.[16] 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.[17] Certain commercial businesses collect this information and create a consumer profile

---

[8] *Id.*
[9] *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 3, 2023).
[10] *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 3, 2023).
[11] *Id.*
[12] 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 3, 2023).
[13] 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 3, 2023).
[14] 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 3, 2023).
[15] 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 3, 2023).
[16] *Id.*
[17] 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 3, 2023).

that describes possible interests or characteristics, and ultimately target ads for their products at the consumer.[18] Other companies—data brokers—collect and sell or share consumer data as their main business operation.[19]

Generally, the types of consumer data that businesses collect are:[20]

- 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).[21] However, no federal law exists that comprehensively regulates how entities across all industries collect and use consumer data.[22] States have recently begun to legislate more comprehensively to protect data privacy.[23]

**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).[24] 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.[25]

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

---

[18] *See supra*, note 10

[19] 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 3, 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 3, 2023).

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

[21] 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 3, 2023).

[22] 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 3, 2023).

[23] 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 3, 2023).

[24] *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 3, 2023).

[25] GDPR, art. 3.

through which an individual can be directly or indirectly identified.[26] 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.[27]

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.[28] This report must be provided to the individual within one month of his or her request.[29] 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.[30]

**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.[31] The CCPA grants consumers greater control over their personal information by, among other provisions, creating the following consumer rights, to:[32]

- Know about the personal information that a business collects, specifically about the consumer, and how it is used and shared;
- 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 business 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:[33]

- Have a gross annual revenue of over $25 million;

---

[26] 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 3, 2023).

[27] 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 3, 2023).

[28] 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 3, 2023).

[29] GDPR, arts. 12(3), 15.

[30] U.K. Information Commissioner's Office, *Guide to General Data Protection Regulation: Right to Erasure, available at* Right to erasure | ICO (last visited April 3, 2023).

[31] Cal. Civ. Code § 1798.140(v)(1).

[32] 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 3, 2023).

[33] Cal. Civ. Code § 1798.140.

- 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.[34]

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:[35]
- 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.[36]

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.[37]

***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.[38] The Virginia Act

[34] Cal. Civ. Code ss. 1798.130, 1798.135.
[35] 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 3, 2023).
[36] *Id*.
[37] 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 3, 2023).
[38] 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 3, 2023).

defines "consumer" only as a natural person who is a resident of Virginia and acts only in an individual or household context.[39]

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.[40]

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.[41] 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.[42]

The Virginia Attorney General has exclusive authority to enforce the Virginia Act.[43]

***Colorado Privacy Act***

The Colorado Privacy Act (Colorado Act) will take effect on July 1, 2023.[44] Generally, with regard to personal data, the Colorado Act grants a consumer the right to:[45]

- Access data;
- 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:[46]

- Control or process personal data of 100,000 or more consumers during a calendar year; or

---

[39] Va. Code Ann. § 59.1-571 (2020).
[40] Va. Code Ann. § 59.1-572 A (2020).
[41] Va. Code Ann. § 59.1-572 B (2020).
[42] Va. Code Ann. § 59.1-572 C (2020).
[43] *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 3, 2023).
[44] C.R.S. 1-6-1301-1313, *available at* https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf (last visited April 3, 2023).
[45] 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 3, 2023).
[46] *Id*.

- 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.[47]

***Utah Consumer Privacy Act***

The Utah Consumer Privacy Act (UCPA) will take effect on December 31, 2023.[48] 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.[49]

Unlike the CCPA, the Colorado Act, and the Virginia Act, the UCPA does not provide consumers with the ability to correct personal data.[50] 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.[51]

The UCPA does not provide a private right of action. The Utah Attorney General will enforce the law.[52]

***Florida Information Protection Act (FIPA)[53]***

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[54] 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

[47] 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 3, 2023).
[48] 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 3, 2023).
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] 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).
[54] 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.

Affairs (DLA).[55] If the breach affected more than 1,000 individuals in Florida, the entity must also notify credit reporting agencies, with certain exceptions.[56]

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.[57]

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.[58]

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).[59] 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.

---

[55] 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 3, 2023). Section 501.171(3)-(4), F.S.
[56] Section 501.171(3)-(6), F.S.
[57] Section 501.171(1)(g)1., F.S.; OAG *supra* note 41.
[58] Section 501.171(1)(g)2., F.S.
[59] Section 501.171(9), (10), F.S.; OAG *supra* note 41.

Under BIPA, a private entity:[60]

- 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.[61]

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.[62] 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.[63]

**Federal Privacy Regulations**

***Health Insurance Portability and Accountability Act (HIPAA)[64] 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.[65]

The Privacy Rule addresses the use and disclosure of individual's protected health information (PHI) by covered entities.[66, 67] 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;

---

[60] 740 Ill. Comp. Stat. 14/10, 14/15 (2008).
[61] 740 Ill. Comp. Stat. 14/20 (2008).
[62] *See Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.
[63] *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).
[64] 42 U.S.C. § 1320.
[65] *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 3, 2023).
[66] 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 3, 2023).
[67] 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.

- 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).[68] 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.

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.[69] 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.[70]

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.[71]

---

[68] 45 C.F.R. §164.302-318.
[69] 21 C.F.R. §§ 50, 60.
[70] *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 3, 2023).
[71] International Council for Harmonisation, *available at* https://www.ich.org/ (last visited April 3, 2023).

***Fair Credit Reporting Act (FCRA)[72]***

The FCRA promotes the accuracy, fairness, and privacy of information that consumer reporting agencies and their related entities collect.[73] 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.[74]

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 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.[75]

***Gramm-Leach Bliley Act (GLBA)[76]***

The GLBA governs financial institutions' use and protection of nonpublic personal information (NPI).[77] 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.[78]

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

---

[72] 15 U.S.C. §1681.

[73] 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 3, 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 3, 2023).

[74] 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).

[75] 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).

[76] 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 3, 2023).

[77] 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).

[78] Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule: Who Must Comply?*, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last visited April 3, 2023).

send an annual notice to the consumer that clearly and conspicuously describes the institution's privacy policies and practices.[79]

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.[80]

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)[81]***

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:

- 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.[82]

COPPA further requires covered entities to:[83]

- Give parents direct notice of their privacy policies, including a description of their data collection and sharing practices;

---

[79] 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.
[80] *See*, 16 C.F.R. § 314.4
[81] 16 C.F.R. pt. 312.
[82] 15 U.S.C. §§ 6502(a)-(b).
[83] *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 3, 2023).

- 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.[84]

***Driver's Privacy Protection Act (DPPA)[85]***

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.

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.[86]

***Family Educational Rights and Privacy Act (FERPA)[87]***

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.[88]

---

[84] 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 3, 2023).
[85] 18 U.S.C. §2721.
[86] 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 3, 2023).
[87] 20 U.S.C. §1232(g); 34 C.F.R. § 99.
[88] 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 3, 2023).

***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.[89] 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.[90]

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.[91]

## III. Effect of Proposed Changes:

**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.

SB 262 creates s. 112.23, F.S., to prohibit 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;
- An attempt to remove content or 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 public safety.

---

[89] 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 3, 2023).

[90] 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 3, 2023).

[91] *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 3, 2023); and Complaint *In the Matter of Sears Holdings Mgmt Co.*, No. C-4264 (F.T.C. Aug. 31, 2009).

**Consumer Data Privacy**

The bill creates s. 501.173, F.S., to establish specific consumer rights over their personal information when held by specific controllers or processors, including:

- The right to access personal information that is collected about the individual consumer;
- The right to delete or correct their personal information; and
- The right to opt-out of the sale or sharing of their personal information with third parties.

A "consumer," as defined by the bill, may exercise these rights. A consumer is any natural person who resides in, or is domiciled in, Florida and who acts in his or her personal capacity or household[92] context. The bill does not contemplate individuals who act in a commercial or employment context.

A controller that receives a verifiable consumer request to access, delete, correct, or opt-out must comply with the request, with certain exceptions.

***Personal Information***

The bill defines personal information as information, including biometric, genetic, and unique identifiers, that is linked, or reasonably capable of being linked, with a particular consumer or household. The term includes:

- Identifiers such as a real name, alias, postal address, unique identifier,[93] online identifier, internet protocol address, email address, account name, social security number, driver license number, passport number, or other similar identifiers;
- Information that identifies, relates to, or describes, or could be associated with, a particular individual, including, but not limited to, a name, signature, social security number, physical characteristics or description, address, location, telephone number, passport number, driver license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information;
- Characteristics of protected classifications under state or federal law;
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information; and
- Inferences drawn from any of the information used to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

[92] The bill defines "household" as a natural person or a group of peole in Florida who reside at the same address, share a common device or the same service provided by a controller, and are identified by a controller as sharing the same group account or unique device.

[93] The bill defines "unique identifier" as a persisitent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or a family, over time and across different services.

The term does not include:

- Consumer employment contact information and similar information that is used only in an employment context;
- De-identified consumer information or aggregate consumer information; and
- Publicly and lawfully available information reasonably believed to be made available to the general public in a lawful manner and without legal restrictions.

***Business Requirements***

*Controllers*

A controller subject to the bill is any sole proprietorship partnership, limited liability company, corporation, association, or legal entity that:

- Is organized or operated for the profit or financial benefit of its shareholders or owners;
- Does business in Florida;
- Collects consumer personal information, or is the entity that directs such collection;
- Determines the purpose and means of processing personal information about consumers, alone or jointly with others;
- Makes in excess of $1 billion in gross revenues, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index; and
- Satisfies one of the following:
    - Derives 50 percent or more of its global annual revenues from providing targeted advertising[94] or the sale of ads online; or
    - 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.[95]

Additionally, any entity that controls or is controlled by a controller is considered a controller for the purposes of the bill.

*Processors*

A processor is a for-profit business that processes information on behalf of a controller pursuant to a written contract. The contract between the controller and processor must prohibit the processor from retaining, using, or disclosing the information for any reason other than that stated in the contract, and as permitted by the bill.

A processor can only act pursuant to a contract between it and the controller. The contract must include provisions that:

- Prohibit the processor from selling, sharing, retaining, using, or disclosing the personal information for any purpose that violates s. 501.173, F.S.;
- Prohibit the processor from retaining, using, or disclosing the personal information other than for the purposes specified in the contract or agreement;

[94] The bill defines "targeted advertising" as marketing to a consumer or displaying an advertisement to a consumer when the advertisement is selected based on personal information used to predict such consumer's preferences or interests.
[95] The bill clarifies that 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.

- Prohibit the processor from combining the personal information that the processor receives from or on behalf of the controller with personal information that the processor receives from or on behalf of another person or that the processor collects from its own interaction with the consumer, provided that the processor may combine personal information to perform any purpose specified in the contract or agreement and such combination is reported to the controller;
- Govern the processor's personal information processing procedures with respect to processing performed on behalf of the controller, including processing instructions, the nature and purpose of processing, the type of information subject to processing, the duration of processing, and the rights and obligations of the controller and processor;
- Require the processor to return or delete all personal information under the contract to the controller as requested by the controller at the end of the provision of services, unless retention of the information is required by law; and
- Require the processor to make available to the controller all personal information in its possession under the contract or agreement, pursuant to the controller's request.

Additionally, the bill provides that determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination. A contract between a controller and processor must reflect their respective roles and relationships related to handling personal information.

If the processor engages a subcontractor, it must require it to meet the same obligations it is required to meet under the bill.

*Third Parties*

A third party is any person who is neither a controller, nor a processor. This may include subcontractors required to engage in data processing, security auditors, or entities that partner with web retail sites to allow consumers to pay in installments.

A third party is prohibited from selling or sharing personal information about a consumer unless the consumer is provided an opportunity by such third party to opt out.
A third party that has collected personal information from a controller in accordance with the requirements in this bill, may use such personal information to advertise or market products or services that are produced or offered directly by such third party.

A third party that engages a subcontractor must require it to meet the same obligations it is required to meet under the bill.

*General Business Obligations*

Generally, a controller that buys, sells, or shares Florida consumers' personal information is subject to the bill. The *sale* of personal information includes the transfer by any means, for actual monetary or valuable consideration, of consumer personal information by a controller to another controller or a third party. In contrast, a controller *shares* consumer personal information when it transfers it by any means, or allows access to it, *for the purpose of advertising or marketing*. The bill specifically includes in its definition of "sharing" (1) allowing a third party to advertise or market to a consumer based on the consumer's personal information, without the disclosure of

the personal information to the third party, and (2) transactions between a controller and third party for advertising and marketing.

*General Exemptions from Provisions of the Bill*
Controllers, processors, and third parties may be exempt from the duties created by the bill, depending on the manner in which they use consumer personal information.

The bill does not apply to the collection of personal information:
- Used for transactional payments;
- Deidentified or aggregate consumer information;
- In compliance with federal, state, or local laws;
- In compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
- In cooperation with law enforcement agencies concerning conduct reasonably believed to violate laws;
- For the purpose of exercising or defending legal rights, claims, or privileges;
- Collected through direct interactions with the consumer, which is used for advertising or marketing services to advertise or market products or services that are produced or offered directly by the controller;
- Pertaining to a job applicant, employee, owner, director, officer, contractor, volunteer, or intern of a controller, to the extent the personal information is collected and used solely within the context of the person's role or former role with the controller;
- Pertaining to protected health information for purposes of the federal Health Insurance Portability and Accountability Act (HIPPA) of 1996 and related regulations;
- By 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 45 C.F.R. parts 160 and 164, or a program or a qualified service program defined in 42 C.F.R. part 2;
- For purposes of research as defined in 45 C.F.R. s. 164.501, conducted in accordance with the Federal Policy for the Protection of Human Subjects for purposes of 45 C.F.R. part 46, the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, or the Protection for Human Subjects for purposes of 21 C.F.R. Parts 50 and 56; or personal information used or shared in research conducted in accordance with one or more of these standards;
- For purposes of compliance with the federal Health Care Quality Improvement Act of 1986 and related regulations, or patient safety work product for purposes of 42 C.F.R. part 3, established pursuant to 42 U.S.C. s. 299b-21 through 299b-26;
- Is deidentified in accordance with 45 C.F.R. part 164 and that is derived from individually identifiable health information, as described in HIPAA, or identifiable personal information, consistent with the Federal Policy for the Protection of Human Subjects or the human subject protection requirements of the United States Food and Drug Administration;
- Used only for public health activities and purposes as described in 45 C.F.R. s. 164.512;
- That is collected, processed, sold, or disclosed pursuant to the federal Fair Credit Reporting Act, 15 U.S.C. s. 1681 and its implementing regulations;
- That is nonpublic personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq. and implementing regulations;

- By a financial institution, as defined in the Gramm-Leach-Bliley Act, 15 U.S.C. ss. 6801 et seq.;
- That is collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et. seq.;
- That consists of education information covered by the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part 99;
- That is collected as part of public or peer-reviewed scientific or statistical research in the public interest and which adheres to all other applicable ethics and privacy laws, if the consumer has provided informed consent;
- Disclosed for the purpose of responding to an alert of a present risk of harm to a person or property or prosecuting those responsible for such activity;
- Disclosed when a consumer uses or directs a controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party;
- That is an identifier used for a consumer how has opted out of the sale or sharing of the consumer's personal information for the sole purpose of alerting processors and third parties that the consumer has opted out of the sale or sharing of the consumer's personal information;
- Transferred by a controller 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;
- Necessary to fulfill the terms of a written warranty when such warranty was purchased by the consumer or the product that is warranted was purchased by the consumer;
- Necessary for a product recall for a product purchased or owned by the consumer conducted in accordance with federal law;
- Processed solely for the purposed of independently measuring or reporting advertising or content performance, reach, or frequency pursuant to a contract with a controller that collected personal information in accordance with this bill;
- Shared between a manufacturer of a tangible product and authorized third party distributors or vendors of the product, as long as such information 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.

*Online Privacy Policy*

Controllers that collect personal information about a consumer must maintain a current online privacy policy that is available on the controller's homepage.[96] The privacy policy must include:

- Any Florida-specific consumer privacy rights;
- The types and categories of personal information that they collect, sell, or share, or have collected, sold, or shared in the past about consumers;
- The consumer's right to request deletion or correction of certain personal information; and

[96] The bill defines "homepage" as the introductrory page of an Internet website and any Internet webpage where personal information is collected. In the case of a mobile application, the homepage is the application's platform page or download page, a link within the application, such as "About" or "Information" application configurations, or the settings page, and any other location that allows consumers to review the notice required by the bill, but not limited to, before downloading the application.

- The consumer's right to opt out of the sale or sharing of their personal information to third parties.

A controller that collects personal information must at or before the point of collection, inform the consumer of the categories of personal information that it will collect, and the purposes for which the categories of information will be used. Additionally, such controllers cannot expand the scope of their collection of personal information or use that personal information outside of its initially expressed purpose without first providing the consumer with additional notice consistent with the requirements of the bill.

*Notice of Retention of Personal Information*

A controller must adopt and implement a retention schedule that prohibits the use or retention of personal information 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.

The retention schedule requirement does not apply to personal information that is reasonably used or retained to do any of the following:

- Fulfill the terms of a written warranty or product recall conducted in accordance with federal law;
- 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;
- Detect security threats or incidents; protect against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecute those responsible for such activities.
- Debug to identify and repair errors that impair existing functionality;
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public's interest that adheres to all applicable ethics and privacy laws when the controller's deletion would likely render impossible or seriously impair the achievement of the research, if the consumer first provided informed consent;
- Enable internal uses that are reasonably aligned with the expectations of the consumer based on the relationship with the controller or that are compatible with the context in which the consumer gave the information;
- Comply with a legal obligation, including any state or federal retention laws;
- Protect the controller's interest against existing disputes, legal actions, or governmental investigations; or
- Assure the physical security of persons or property.

*Data Security*

A controller that collects a consumer's personal information must implement and maintain reasonable security procedures and practices to protect personal information from unauthorized or illegal access, destruction, use, modification, or disclosure. Additionally, a controller must

require any processors to implement and maintain the same or similar security procedures and practices.

***Consumer Rights Based on the Sale of Personal Information***

The bill establishes specific consumer rights regarding their personal information, including:
- The right to access personal information that was collected about them;
- The right to delete or correct their personal information; and
- The right to opt-out of the sale or sharing of their personal information with third parties.

The bill prohibits as contrary to public policy any waiver or limitation of a consumer's rights as provided by the bill, including the waiver or limitation of the consumer's right to a remedy or means of enforcement.

*Verifiable Requests*

A consumer must make a verifiable request to exercise their rights to know, delete, or correct, their collected personal information.

A "verifiable consumer request" is defined as a request that is submitted to a controller by:
- A consumer;
- A parent or guardian on behalf of a consumer who is a minor child; or
- A person authorized by the consumer to act on the consumer's behalf.

A verifiable consumer request is presumed to have been made when requested through an established account using the controller's established security features to access the account through communication features offered to consumers. However, a controller may not require the consumer to create or have an account with the controller in order to make a verifiable consumer request.

***Right to Request a Copy of Personal Information that is Collected, Sold, or Shared***

The bill grants consumers the right to request an accounting of certain information from a controller who collects, sells, or shares their personal information. Within 45 calendar days of its receipt of the request, the controller must respond with the following information in a readily usable format:
- The specific pieces of personal information collected about the consumer;
- The categories of sources from which the consumer's personal information was collected;
- The specific pieces of personal information about the consumer that were sold or shared;
- The third parties to which the controller sold or shared the consumer's personal information; and
- The categories of consumer personal information that were disclosed to a processor.

The controller may extend their response period by an additional 45 calendar days (for a total of 90 calendar days) if they inform the consumer of the extension within the first 45 days from receipt of the request. This right does not apply to information that relates solely to households.

Additionally, the controller is not required to provide the above-requested information more than twice in a 12-month period.

This right to request a copy of personal information does not otherwise require controllers to retain, reidentify, or link data that they would not maintain in their ordinary course of business. Additionally, a controller is permitted to provide the data to the consumer in a manner that does not disclose the controller's trade secrets.

*Right to Delete and Correct Personal Information*

A consumer may request that a controller delete personal information that it collected about the consumer or about the consumer's child younger than 18 years old. After the business receives such a request, it must delete the information and direct any processors the delete the information within 90 days.

A consumer may request to correct personal information about the consumer or about the consumer's child younger than 18 years old that is held by a controller. The controller must use commercially reasonable efforts to correct the inaccurate information as directed by the consumer and direct any processor to correct it as well within 90 days of the request. A controller can allow a consumer to correct information through a self-service mechanism.

Controllers and processors acting pursuant to a contract with the controller are not required to comply with a request to delete or correct information if it is necessary to:

- Complete the transaction for which the personal information was collected;
- Fulfill the terms of a written warranty or product recall that is conducted in accordance with federal law;
- Detect security threats or incidents; protect against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecute those responsible for such activity;
- Debug and identify repair errors;
- Engage in public or peer-reviewed scientific, historical, or statistical research that is performed in accordance with applicable ethical standards and privacy laws—only when the deletion of the consumer's personal information would render such research impossible or seriously impaired and where the consumer previously provided informed consent;
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller;
- Comply with a legal obligation, including state or federal retention laws;
- Reasonably protect the controller's interests against existing disputes, legal action, or governmental investigation; or
- Assure the physical security of persons or property.

Additionally, a controller and contracted-processor are not required to comply with a request to delete a consumer's personal information if it is required to:

- Provide a good or service requested by the consumer, or reasonably anticipate the request of a good or service within the context of the controller's ongoing business relationship with the consumer, or otherwise perform a contract between the controller and consumer; or

- Engage in public or peer-reviewed research that adheres to applicable ethics and privacy laws, if the deletion would likely render impossible, or seriously impair the research, and if the consumer initially provided informed consent.

***Right to Opt Out of the Sale or Sharing of Personal Information***

The bill creates a "right to opt out," which allows a consumer to instruct a controller that sells personal information to a third party not to sell their personal information. A controller must stop selling and sharing the consumer's personal information within 4 calendar days after it receives an opt-out request, and cannot begin to sell or share the consumer personal information again unless it receives subsequent express authorization. Additionally, a controller is prohibited from selling or sharing the personal information of a minor consumer if the controller has actual knowledge that the consumer is not at least 18 years old. However, if a consumer who is between 13 and 18 years old, or if the parent or guardian of a consumer who is 12 years old or younger, has affirmatively authorized the sale or sharing of such consumer's personal information, then a controller may do so pursuant to the requirements under the bill.

The controller must provide a clear and accessible link on its homepage to consumer's entitled "Do Not Sell or Share My Personal Information" to allow the consumer to opt out. The controller cannot require a consumer to create an account. A consumer's opt out request may also be made through a user-enabled global privacy control, e.g., a browser plug-in or privacy setting. Any personal information collected from the consumer in connection with an opt out request must solely be used to comply with such request. Additionally, a consumer may authorize another person to opt out on the consumer's behalf.

The controller must respect the consumer's opt out request for at least 12-months before it can request the consumer's authorization of the sale or sharing of consumer personal information again.

*Incentives for Consent to Sell or Share Personal Information*

A controller cannot deny goods or services to a consumer because the consumer exercised any rights under the bill.

A controller can charge a consumer who exercised any of the rights granted by the bill a different price or rate, or provide a different level or quality of goods or services to the consumer, only if that difference is:

- Reasonably related to the value provided to the controller by the consumer's data, or
- Related to a consumer's voluntary participation in a financial incentive program, including loyalty, rewards, premium features, discounts, or club card program that is offered by the controller.

A controller can offer additional benefits to consumers who participate in the collection, sharing, sale, or deletion of personal information. This consent must have been granted based on a clear description of the material terms of the incentive program, and the consumer must be permitted to revoke his or her consent at any time. The discount or promotional item must be reasonably

related to the value the consumer's data provides to the business and must not be unjust, unreasonable, coercive, or usurious.

**Surveillance**

A controller is prohibited from collecting a consumer's precise geolocation data or personal information through the operation of a voice recognition feature, unless the consumer provides authorization.

Precise geolocation data is information from technology, such as global positioning system level latitude and longitude coordinates or other mechanisms, which directly identifies the specific location of a person within a radius of 1,750 feet. However, the term does not include information generated by the transmission of communications or any information generated by or connected to advance utility metering infrastructure systems.

A 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.

**Search Engine Transparency**

A controller that operates a search engine must provide a consumer with information of how the controller's search engine algorithm prioritizes or deprioritizes political partisanship or political ideology in its search results.

**Agency Enforcement and Implementation**

The Department of Legal Affairs (DLA) may prosecute on behalf of a Florida consumer any violation of the bill's provisions as a deceptive and unfair trade practice, pursuant to the Florida Deceptive and Unfair Trade Practices Act (FDUTPA).[97]

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;[98]
- Award actual damages based on the violation;[99]
- Award a civil penalty of not more than $50,000 for each willful violation; and
- Triple the civil penalty if the violation:

[97] For the purpose of brining an action pursuant to this bill ss. 501.211 and 501.212, F.S., do not apply.
[98] Section 501.207(1), F.S.
[99] Section 501.207(1), F.S.

- Involves a Florida consumer who the controller, processor, or third party has actual knowledge is 18 years of age or younger, or
- Is based on a controller's, processor's, or third party's failure to delete or correct the consumer's personal information after receiving a verifiable 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 verifiable 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.

The bill requires 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.

***Report by the Department of Legal Affairs***

The bill requires the DLA to submit a report by February 1 each year to the President of the Senate and the Speaker of the House of Representatives 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
- The status of the development and implementation of rules to implement the bill.

**Preemption**

The bill provides 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**

The bill amends s. 501.171, F.S., to define "biometric information" as an individual's physiological, biological, or behavioral characteristics that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. The term includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a face print, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

The bill defines **"**genetic information**"** as an individual's deoxyribonucleic acid (DNA).

The bill includes biometric information, genetic information, and 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.

**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:

## 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 and 501.173.

## IX. Additional Information:

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

None.

B. Amendments:

None.