

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: CS/SB 1734

INTRODUCER: Commerce and Tourism Committee and Senator Bradley

SUBJECT: Consumer Data Privacy

DATE: March 23, 2021

REVISED: _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McKay	CM	Fav/CS
2.			AP	
3.			RC	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 1734 creates the Florida Privacy Protection Act (Act) to grant Florida’s consumers the ability to share their personal information as they wish, in a way that is safe and that they understand and control.

The Act generally applies to businesses that collect Florida consumers’ personal information, and that either have a gross revenue of \$25 million or more; earn 50 percent of their revenue from the sale or sharing of personal information; or buy, receive, sell, or share the personal information of 50,000 or more consumers in a year.

The Act grants consumers the right to:

- Opt-out of the sale of their personal information;
- Know what personal information a business has collected about them;
- Delete their personal information;
- Correct their personal information;
- More stringently control the sale of their minor child’s personal information.

Businesses subject to the Act must give consumers notice of their privacy rights, that their personal information may be sold and collected, and that the consumer may opt-out of the sale of his or her personal information. A consumer’s opt-out would prevent the sale of his or her data to third-party data brokers, data profiling procedures, and targeted advertisements based on the consumer’s activity at more than one website. Additionally, the act requires covered businesses

to implement data security measures to ensure the continued privacy of the personal information they hold.

A consumer may pursue a private civil action based on a business' violation of the Act. The Florida Department of Legal Affairs also has enforcement authority pursuant to the bill.

The bill takes effect on January 1, 2022.

II. Present Situation:

Americans are concerned about how much of their data is being collected, and many feel that their information is less secure than it used to be.¹ Further, 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.² Despite this concern—very few read provided privacy policies in full, if at all.³

Consumer internet connectivity has increased in recent years, allowing consumer data to be collected not only from a personal computer, but also a smartwatch, phone, smart speaker, and even a home appliance.⁴ It is expected that the value of such connected devices and “the ecosystem in which they operate” will exceed four trillion dollars per year by 2025.⁵

Consumer data is most commonly tracked through the placement of ‘cookies’—files that a website places in the user’s device—or more sophisticated “fingerprinting” techniques.⁶ These technologies allow websites to, e.g., store a password that a consumer previously entered, but also allow websites 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.⁷ Certain commercial businesses collect this information and create a consumer profile that describes

¹ Brooke Auxier and Lee Rainie, PEW RESEARCH CENTER, *Key Takeaways on Americans’ Views About Privacy, Surveillance and Data-Sharing* (Nov. 15, 2019), <https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/> (last visited Mar. 23, 2021). *See also*, 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 2 (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 Mar. 23, 2021).

² Auxier, et. al, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over their Personal Information* at 7.

³ *Id.* at 5.

⁴ *See, e.g.*, Oracle, *What is IoT [Internet of Things]?*, <https://www.oracle.com/internet-of-things/what-is-iot/> (last visited Mar. 23, 2021). Stephen Mulligan, Wilson Freeman, Chris Linebaugh, Congressional Research Service, *Data Protection Law: An Overview* at 1 (Mar. 25, 2019), <https://crsreports.congress.gov/product/pdf/R/R45631> (last visited Mar. 23, 2021).

⁵ Commissioner Rebecca K. Slaughter, Federal Trade Commission, *Raising the Standard: Bringing Security and Transparency to the Internet of Things?* (July 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter_-_raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf (last visited Mar. 23, 2021).

⁶ NPR.ORG, *Online Trackers Follow our Digital Shadow by ‘Fingerprinting’ Browsers, Devices* (Sep. 26, 2016), <https://www.npr.org/sections/alltechconsidered/2016/09/26/495502526/online-trackers-follow-our-digital-shadow-by-fingerprinting-browsers-devices> (last visited Mar. 23, 2021).

⁷ Wharton School of Business, University of Pennsylvania, *Your Data is Shared and Sold... What’s Being Done About It?* (Oct. 28, 2019), <https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/> (last visited Mar. 23, 2021).

possible interests or characteristics, and ultimately target ads for their products at the consumer.⁸ Other companies—data brokers—collect and sell consumer data as their main business operation.⁹

Policy regarding consumer data has two prongs: privacy and security. Data privacy concerns how companies collect, use, and disseminate personal information; data security concerns how companies protect the personal information they hold from unauthorized access or use and respond to such breaches.¹⁰ 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).¹¹ States have recently begun to legislate more comprehensively to protect data privacy.¹²

Florida Information Protection Act (FIPA)¹³

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 entities¹⁴ 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).¹⁵ If the breach affected more than 1,000 individuals in Florida, the entity must also notify credit reporting agencies, with certain exceptions.¹⁶

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;

⁸ Max Freedman, BUSINESS NEWS DAILY, *How Businesses are Collecting Data (and What They’re Doing With It)* (Jun. 17, 2020), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html> (last visited Mar. 23, 2021).

⁹ Lois Beckett, PROPUBLICA, *Everything We Know About What Data Brokers Know About You* (June 13, 2014), <https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you> (last visited Mar. 23, 2021).

¹⁰ See, e.g., Andrew Burt and Dan Geer, *Data Protection for the Disoriented, From Policy to Practice* 9 (2018), available at <https://www.lawfareblog.com/flat-light-data-protection-disoriented-policy-practice> (last visited Mar. 23, 2021).

¹¹ Stephen Mulligan, Wilson Freeman, Chris Linebaugh, Congressional Research Service, *Data Protection Law: An Overview* at 7-8 (Mar. 25, 2019), <https://crsreports.congress.gov/product/pdf/R/R45631> (last visited Mar. 23, 2021).

¹² NCSL, *2020 Consumer Data Privacy Legislation* (Jan. 17, 2020), <https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx> (last visited Mar. 23, 2021).

¹³ 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).

¹⁴ 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.

¹⁵ Florida Office of the Attorney General, *How to Protect Yourself: Data Security*, <http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C> (last visited Mar. 23, 2021). Section 501.171(3)-(4), F.S.

¹⁶ Section 501.171(3)-(6), F.S.

- 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; or
- Medical history information or health insurance identification numbers.¹⁷

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.¹⁸

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).¹⁹

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.

Federal Privacy Regulations

*Gramm-Leach Bliley Act (GLBA)*²⁰

The GLBA governs financial institutions' use and protection of nonpublic personal information (NPI).²¹ 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.²²

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

¹⁷ Section 501.171(1)(g)1., F.S.; OAG *supra* note 15.

¹⁸ Section 501.171(1)(g)2., F.S.

¹⁹ Section 501.171(9), (10), F.S.; OAG *supra* note 15.

²⁰ 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), <https://crsreports.congress.gov/product/pdf/R/R45631> (last visited Mar. 23, 2021).

²¹ 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).

²² Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule: Who Must Comply?*, <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying> (last visited Mar. 23, 2021).

send an annual notice to the consumer that clearly and conspicuously describes the institution's privacy policies and practices.²³

The financial institution must also ensure the security and confidentiality of a customer's (which requires an ongoing relationship with the financial institution) NPI by establishing concrete security policies, by, e.g., designating an information security program coordinator and implementing a risk assessment process.²⁴

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.

Health Insurance Portability and Accountability Act (HIPAA)²⁵ 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.²⁶

The Privacy Rule addresses the use and disclosure of individual's protected health information (PHI) by covered entities.^{27, 28} 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 de-identified 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

²³ 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.

²⁴ See, 16 C.F.R. § 314.4

²⁵ 42 U.S.C. § 1320.

²⁶ See generally, Stephen Mulligan, Wilson Freeman, Chris Linebaugh, Congressional Research Service, *Data Protection Law: An Overview* pp. 10-12 (Mar. 25, 2019), <https://crsreports.congress.gov/product/pdf/R/R45631> (last visited Mar. 23, 2021).

²⁷ 45 C.F.R. §160 and 164. See also, Department of Health and Human Services, *Summary of the HIPPA Privacy Rule*, (Jul. 26, 2013) <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Mar. 23, 2021).

²⁸ 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.

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).²⁹ 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 impermissible 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.³⁰ Twenty 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.³¹

Fair Credit Reporting Act (FCRA)³²

The FCRA promotes the accuracy, fairness, and privacy of information that consumer reporting agencies and their related entities collect.³³ 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.

²⁹ 45 C.F.R. §164.302-318.

³⁰ 21 C.F.R. §§ 50, 60.

³¹ See generally, Health and Human Services, *Federal Policy for the Protection of Human Subjects ('Common Rule')* (Mar. 18, 2016), <https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html> (last visited Mar. 23, 2021).

³² 15 U.S.C. §1681.

³³ Consumer Finance Bureau, *A Summary of Your Rights Under the Fair Credit Reporting Act* (Sept. 18, 2018), 12 CFR 1022, available at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> (last visited Mar. 23, 2021). See also, Federal Trade Commission, *Fair Credit Reporting Act*, <https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act> (last visited Mar. 23, 2021).

A CRA cannot provide information in a consumer report to anyone who does not have a specified purpose in the FCRA.³⁴

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.³⁵

Children's Online Privacy Protection Act (COPPA)³⁶

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.³⁷

COPPA further requires covered entities to:³⁸

- 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;

³⁴ 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).

³⁵ 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).

³⁶ 16 C.F.R. pt. 312.

³⁷ 15 U.S.C. §§ 6502(a)-(b).

³⁸ See, Federal Trade Commission, *General Questions About the COPPA Rule: What is the Children's Online Privacy Protection Rule?*, <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0> (last visited Mar. 23, 2021).

- 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 deemed an unfair or deceptive act or practice and are therefore 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.³⁹

Driver’s Privacy Protection Act (DPPA)⁴⁰

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.⁴¹

Family Educational Rights and Privacy Act (FERPA)⁴²

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.⁴³

³⁹ Federal Trade Commission, *General Questions About the COPPA Rule: COPPA Enforcement*, <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0> (last visited Mar. 23, 2021).

⁴⁰ 18 U.S.C. §2721.

⁴¹ 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*, <https://epic.org/privacy/drivers/> (last visited Mar. 23, 2021).

⁴² 20 U.S.C. §1232(g); 34 C.F.R. § 99.

⁴³ U.S. Department of Education, *Family Educational Rights and Privacy Act (FERPA)*, (Dec. 15, 2020) <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html> (last visited Mar. 23, 2021).

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.⁴⁴ 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.⁴⁵

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.⁴⁶

The FTC generally cannot seek civil penalties for violations of the FTC Act, but may assess civil monetary penalties for repeated offenses.⁴⁷ There is no private right of action granted under the FTC Act.

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).⁴⁸ 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.⁴⁹

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.⁵⁰ A processor and controller must receive express consent from an individual before they can collect or process his or her

⁴⁴ 15 U.S.C. § 1681. Federal Trade Commission, Privacy and Security Enforcement, <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited Mar. 23, 2021).

⁴⁵ Stephen Mulligan, Wilson Freeman, Chris Linebaugh, CONGRESSIONAL RESEARCH SERVICE, *Data Protection Law: An Overview* p. 30-35 (Mar. 25, 2019), <https://crsreports.congress.gov/product/pdf/R/R45631> (last visited Mar. 23, 2021).

⁴⁶ 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), <https://crsreports.congress.gov/product/pdf/R/R45631> (last visited Mar. 23, 2021); and Complaint In the Matter of Sears Holdings Mgmt Co., No. C-4264 (F.T.C. Aug. 31, 2009).

⁴⁷ Federal Trade Commission, FTC's Use of Its Authorities to Protect Consumer Privacy and Security at 4 (2020), available at <https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf> (last visited Mar. 23, 2021).

⁴⁸ See generally, Stephen Mulligan, Wilson Freeman, Chris Linebaugh, CONGRESSIONAL RESEARCH SERVICE, *Data Protection Law: An Overview* p. 42 (Mar. 25, 2019), <https://crsreports.congress.gov/product/pdf/R/R45631> (last visited Mar. 23, 2021).

⁴⁹ GDPR, art. 3.

⁵⁰ GDPR, art. 4(1). See, U.K. Information Commissioner's Office, *Guide to General Data Protection Regulation: What is Personal Data?*, <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 Mar. 23, 2021).

personal data. The language must give a clear choice that is not based on an overbroad or overly complex question.⁵¹

The GDPR requires entities subject to the GDPR to provide individuals with a report of their data that is processed, where it is processed, why it is being processed.⁵² This report must be provided to the individual within one month of his or her request.⁵³ 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.

State Data Privacy Regulations

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:⁵⁴

- That possesses biometric data must have a written policy that establishes a retention schedule and guidelines for permanent 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.⁵⁵

The Illinois Supreme Court found that an individual need not 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

⁵¹ U.K. Information Commissioner's Office, *Guide to General Data Protection Regulation: Consent*, <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 Mar. 23, 2021).

⁵² Mark Kaelin, TECHREPUBLIC, *GDPR: A Cheat Sheet* (May 23, 2019), <https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/> (last visited Mar. 23, 2021).

⁵³ GDPR, arts. 12(3), 15.

⁵⁴ 740 Ill. Comp. Stat. 14/10, 14/15 (2008).

⁵⁵ 740 Ill. Comp. Stat. 14/20 (2008).

injunctive relief under BIPA.⁵⁶ 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.⁵⁷

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

The CCPA 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.⁵⁸ The CCPA grants consumers greater control over their personal information by, among other provisions, creating the following consumer rights, to:

- 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:

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

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

The CPRA broadens consumers' rights by allowing them to:

- 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 redefines businesses subject to the law to include those that buy, sell, or share the personal information of 100,000 or more consumers or households; this reduces its applicability

⁵⁶ *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.

⁵⁷ *Rivera v. Google, Inc.*, 238 F.Supp.3d 1088 (N.D. Ill. 2017); *In re Facebook Biometric Information Privacy Litigation*, 185 F.Supp.3d 1155 (N.D. Cal. (2016).; *Norberg v. Shutterfly, Inc.*, 152 F.Supp.3d 1103 (N.D. Ill. 2015).

⁵⁸ Cal. Civ. Code § 1798.140(O)(1).

to small and mid-size businesses. However, CPRA also now applies to businesses that not only sell personal information, but also ones that share it; it is unclear to what extent this will enlarge the businesses captured by the regulation. Additionally, the CPRA now prohibits sharing of data between different entities that make up a joint venture.

The CPRA creates a privacy regulator with implementation and enforcement authority relating to the CCPA and CPRA. The CPRA also increases penalties by allowing civil penalties for the theft of consumer login information and increasing the maximum penalties for violations that concern consumers under the age of 16.

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.⁵⁹

CCPA and the Federal Airline Deregulation Act

The federal Airline Deregulation Act expressly preempts state laws that relate to a price, route, or service of an air carrier.⁶⁰ California brought an action against Delta Airlines for a violation of the CCPA because the airline failed to disclose a privacy policy on its mobile application despite the fact that it collected personally identifiable information about its consumers. This action failed, however, on the basis that the CCPA was preempted by the Airline Deregulation Act.⁶¹

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.⁶² 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.⁶³

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.⁶⁴

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

⁵⁹ 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), <https://www.jdsupra.com/legalnews/the-cpra-s-storage-limitation-9898179/> (last visited Mar. 23, 2021).

⁶⁰ 49 U.S.C.A. § 41713.

⁶¹ *Harris v. Delta Air Lines, Inc.*, 247 Cal. App. 4th 884, 202 Cal. Rptr. 3d 395 (2016). See also, Heather Zachary and Allison Trzop, *Online Consumer Privacy: Airlines Under Scrutiny*, (Jul. 29, 2014) <https://www.wilmerhale.com/en/insights/publications/online-consumer-privacy-airlines-under-scrutiny> (last visited Mar. 23, 2021).

⁶² Va. Code Ann. § 59.1-573 (2020).

⁶³ Va. Code Ann. § 59.1-571 (2020).

⁶⁴ Va. Code Ann. § 59.1-572 A (2020).

public entities, nonprofit organizations, and higher education institutions.⁶⁵ 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.⁶⁶

The Virginia Attorney General has exclusive enforcement authority of the Virginia Act.⁶⁷

	VCDPA	CCPA, as amended by the CPRA	GDPR
Right to opt-out of sale	✓	✓	✗
Opt-in or opt-out for processing of sensitive information	Opt-in	Opt-out	Opt-in
Statutory cure period for violations	✓	✓	✗
Right to appeal denials of requests	✓	✗	✗
Express obligations regarding de-identified data	✓	✗	✗
Requirement to perform data protection impact assessments	✓	✓	✓
Private right of action	✗	✓	✓
Governmental enforcement entities	Attorney General	CPPA, Attorney General	DPA's
Penalties	Up to \$7,500 per violation	Up to \$2,500 per violation and up to \$7,500 per intentional violation or violation involving minors	Up to €10 million, or 2% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of less severe violations. Up to €20 million, or 4% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of more serious violations.
Operative date	January 1, 2023	January 1, 2023	May 25, 2018

68

III. Effect of Proposed Changes:

CS/SB 1734 creates the Florida Privacy Protection Act to grant Florida’s consumers the ability to share their personal information as they wish, in a way that is safe and that they understand and control. The bill grants specific rights to consumers, and regulates businesses that collect, process, or sell personal information about consumers.

⁶⁵ Va. Code Ann. § 59.1-572 B (2020).

⁶⁶ Va. Code Ann. § 59.1-572 C (2020).

⁶⁷ See generally, Kurt Hunt and Matthew Diaz, JDSUPRA, *Virginia Becomes 2nd State to Adopt a Comprehensive Consumer Data Privacy Law* (Mar. 8, 2021), <https://www.natlawreview.com/article/virginia-becomes-2nd-state-to-adopt-comprehensive-consumer-data-privacy-law> (last visited Mar. 23, 2021).

⁶⁸ Briana Falcon and Devika Kornbacher, JDSUPRA, *Virginia is for Lovers...of Data Privacy* (Feb. 15, 2021), <https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3879845/> (last visited Mar. 23, 2021).

Personal Information

The bill defines personal information as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, such as a consumer's:

- First and last name;
- Home or other physical address that includes the name of a street and city or town;
- E-mail address or phone number;
- Social security number;
- Identifier, such as an alias, unique personal identifier, online identifier, Internet protocol (IP) address, account name, driver license number, passport number, or similar identifier;
- Biometric information,⁶⁹ such as DNA or fingerprints or any other biometric information that a business collects about the consumer without his or her knowledge;
- Internet or other electronic network activity information, including but not limited to, browsing and search history, and information regarding a consumer's interaction with a website, application, or advertisement;
- Audio, electronic, visual, thermal, olfactory, geolocation, or similar information;
- Professional or employment-related information;
- Education information, defined as only information that is not publicly available;
- Information that may serve as a probabilistic identifier⁷⁰ concerning him or her which is collected from the consumer through a website, online service, or some other means by the business and is maintained by the business in combination with an identifier that, when used with the information, identifies the consumer;
- Characteristics of protected classifications under state or federal law;
- Commercial information, including records of personal property, purchased or considered products or services, or other purchasing and shopping habits; and
- Geolocation data.

The bill further defines personal information as any inferences drawn from the above information regarding the consumer that can be compiled to create a consumer profile that reflects his or her preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. This list is not exhaustive of information that may constitute personal information.

However, the bill specifies that the definition of personal information *does not* include:

- Information obtained from public records, including information that is lawfully made available from federal, state, or local governmental records;

⁶⁹ The bill defines "biometric information" as "an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), which 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, or palm; vein patterns; voice recordings from which an identifier template, such as a faceprint, a minutiae template, or a voice print, can be extracted; keystroke patterns or rhythms; gait patterns or rhythms; and sleep, health, or exercise data that contain identifying information."

⁷⁰ The bill defines a "probabilistic identifier" as the identification of a consumer or a device to a degree of certainty ... based on categories of personal information included in or similar to a person's personal information.

- Information that was made available to the general public by either the consumer or widely distributed media and that the collecting business has a reasonable basis to believe is lawfully available;
- Information that is truthful and that is a matter of public concern; and
- De-identified consumer information or aggregate consumer information that relates to a group or category of consumers from which individual consumer identities have been removed.

Information is de-identified if it:

- Cannot reasonably identify, relate to, describe, or be associated with or linked to a particular consumer or device;
- Contains data that the business has taken reasonable measures to ensure cannot be reidentified;
- Contains data that the business publicly commits to maintain and use in a de-identified fashion and that it will not attempt to reidentify; and
- Contains data that the business contractually prohibits downstream recipients from attempting to reidentify.

Aggregate consumer information, like de-identified information, has had individual consumer identities removed from it and cannot be linked to any consumer or household—but it relates to a group or category of consumers as a whole, rather than to a particular consumer.

Consumer Rights

The bill defines a consumer as a person who is in Florida for a purpose that is not temporary or transitory. The term specifically excludes nonresidents. A person can be an individual, business, or other organization or group of persons who act in concert. The bill vests consumers with specific rights regarding their personal information in interactions with businesses that collect and sell consumer personal information.

Minor’s Right to Opt-In to the Sale of Personal Information

The bill prohibits a business from *selling* a consumer’s information if he or she is younger than 13 years old, unless the business has affirmative authorization to do so from the child’s parent or guardian. Similarly, a business may not collect the personal information of an individual who is between the ages of 13 and 16 unless he or she has affirmatively opts-in. This “opt-in” right does not prevent businesses from *collecting* the individual personal information of consumers under the age of 16.

A business is deemed to have actual knowledge of its consumers’ ages if it willfully disregards such information, and therefore is subject to penalty under the bill if it fails to institute some method to determine its consumers’ ages. However, what specifically constitutes “willful disregard” of this information will likely need to be determined by a trier of fact.

Right to Opt Out of the Sale of Personal Information

The bill creates a “right to opt out of the sale,” which allows a consumer who is 16 years old, or older to instruct a business that sells personal information not to sell his or her personal

information. The business may not require a consumer to create an account to submit his or her opt out request. As discussed below,⁷¹ “sale” is defined expansively by the bill to include any transfer or communication of consumer personal data to advance a business’ economic interests.

The business must stop selling the consumer’s personal information as soon as reasonably possible, but within no more than 2 days after it receives an opt-out request.

A consumer’s opt-out request may also be made by an authorized third-party or through a user-enabled global privacy control, e.g., a browser plug-in or privacy setting. A business cannot require a consumer to make a verified request to submit his or her request to opt out.

Targeted Advertisements and Profiling

The right to opt-out includes a right to opt-out of the processing of one’s data for the purposes of profiling and targeted advertising.

Profiling is defined as the automated processing that a business performs on a consumer’s personal data that will evaluate or predict things about the consumer’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Targeted advertising is distinct from profiling in result—that it ultimately leads to the display of an advertisement to the consumer based on the profiling of his or her personal data obtained from a broad array of the consumer’s activities, including activity on other business’ websites or applications. As defined by the bill, targeted advertising does not include nonpersonalized advertising that is based only on the consumer’s personal information derived from the consumer’s current interaction with the business—excluding the consumer’s precise geolocation.

A consumer may trigger this specific portion of the right to opt-out at any time, but it is unclear whether he or she must also execute the broader opt-out right to enable the targeted advertisement and profiling opt-out.

A business can offer additional benefits to consumers who participate in targeted advertisements or profiling processes. For example, a business can offer a consumer who participates in targeted advertisements, loyalty programs or related enticements free goods or services, and goods or services at a different price, rate, level, quality, or selection than that offered to consumers who opt out. However, 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.

Duration of opt out

Once a consumer opts out, the business must comply without requiring any additional consumer action if it can identify the consumer through a login protocol or similar process, or if the business is made aware of the consumer’s continued opt-out preference by a user-enabled global privacy control, such as a browser plug-in or privacy setting.

⁷¹ See *infra*, Notice Requirements: Notice of Sale of Personal Information.

The bill states elsewhere that a business that received an opt-out request is prohibited from selling the consumer's personal information until it receives the consumer's subsequent express authorization. Additionally, section 501.175(5)(d) of the bill permits a business to request a consumer to re-authorize his or her opt-out after 12 months have passed from initial receipt of the consumer's preference. The bill therefore appears to provide inconsistent guidance regarding re-authorization of a consumer's opt out request.

Right to Know, Edit, or Delete Specific Collected Public Information

The bill grants consumers several additional rights that revolve around the need to first know what a covered business actually holds about the consumer. These rights are the right to know the details of one's personal information held by a business, the right to correct that personal information, and the right to have it deleted. A consumer must submit a verified request to exercise these rights.

Verified Requests

A consumer must make a verified request to exercise his or her rights to know, delete, or correct their collected personal information. An opt-out or opt-in request is not required to be made by verified request.

A "verified request" is defined as a request that is submitted to a business by one of the following:

- A consumer;
- A consumer on behalf of his or her minor child; or
- A natural person or a person registered with the Secretary of State who is authorized by the consumer to act on his or her behalf.

The business must be able to reasonably verify that the request is authentic.

Businesses must establish a designated request address to which consumers may submit their verified request; the address may be either an e-mail address, toll-free phone number, or website. It appears that businesses may receive verified requests in other manners, as a verified request is not defined as one submitted to a business' designated request address.

The covered business is required to respond to the consumer's verified request to access, correct, or delete personal information within 30 days of its submission. The business may take an additional 30 days (total of 60 days) to respond if it makes a good faith determination that it is reasonably necessary to do so. Any business that extends its response beyond the initial 30-day timeframe must notify the requesting consumer of the extension.

If the business deems the consumer request manifestly unfounded or excessive—especially where the consumer's request is overly repetitive, the business may either refuse to comply or charge a reasonable fee for the services requested. The fee must take into account administrative cost of the work required to respond. If a business refuses to respond, it must notify the consumer of the underlying reason. It is the business' burden to demonstrate that the consumer's verified request was unfounded or burdensome.

Right to an Accounting of One's Personal Information Held by a Covered Business

A consumer has the right to request an accounting of certain information from a covered business.⁷² This information includes:

- The sources from which the business collected the consumer's personal information;
- The specific items of personal information the business collected about the consumer;
- The third parties to whom the business sold the personal information.

However, the corresponding business obligation appears only to require that the business provide "any personal information about the consumer which it has collected, directly or indirectly...". Another portion of the bill requires the business to comply with a consumer's request to "access" personal information.

A separate section of the bill obligates businesses that control the collection of a consumer's personal information that will be used for any purpose other than a business purpose to inform consumers of the purposes for which it collects or uses personal information, as applicable to each category of personal information it collects or uses. These specific businesses must also inform its consumers whether it will sell their personal information. This requirement applies to the general public and does not require specific or personal information to be provided to individuals.

It is therefore unclear whether a consumer's right to request the sources from which his or her personal information was collected and the third parties to which it was sold actually translates to a right to receive such information from a covered business.

A service provider is not required to personally comply with a verified request. It is obligated to provide any personal information it obtained as a result of its performance under a contract with a business to said business in order to help the business respond to a verified request for information.

Because the law cannot be applied retroactively, a business is required to disclose only the information it collected about a consumer since July 1, 2022.

Right to Delete Personal Information

A consumer may submit a verified request that a covered business that sells his or her information delete it. After the business receives such a request, it must delete the information, and instruct any third party that bought or received the consumer's personal information to delete the information.

A business and service provider are not required to delete a consumer's personal information pursuant to his or her request where it is necessary to maintain to:

⁷² It is unclear to what businesses consumers have the right to submit this request. The right is created in a subsection that obligates "businesses required to comply with this section." However, there is no general statement of required compliance within the section. Other subsections within the section apply to businesses that sell consumer information, so this right may also only apply to businesses that sell a consumer's information.

- Complete the transaction, provide the good or service, or perform a contract, 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;
- Ensure the security and integrity of the business, the personal information it holds, or the safety of a natural person;
- Debug and identify repair errors;
- Exercise free speech or another right provided for by law;
- 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; and
- Comply with a legal obligation.

Where a business has already de-identified the personal information, it cannot be required to reidentify it to accommodate a request to delete personal information.

Right to Correct Inaccurate Personal Information

A consumer may submit a verified request that a covered business correct incorrect personal information it holds about him or her. A business and any service provider must correct the incorrect information.

Business Requirements

Covered Businesses

The bill defines a business subject to the Act (covered business) as a sole proprietorship, partnership, limited liability company, corporation, association, or any other legal entity that:

- Is organized or operated for the profit or financial benefit of its shareholders or owners;
- Does business in Florida;
- Collects personal information about consumers, or is the entity on behalf of which such information is collected;
- Determines the purpose and means of processing personal information about consumers, alone or jointly with others; and
- Satisfies at least one of the following thresholds:
 - Has a global annual gross revenue in excess of \$25 million, as adjusted in January of every odd-numbered year to reflect an increase in the consumer price index;
 - Annually buys, receives for the business’ commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices; or
 - Derives 50 percent or more of its global annual revenues from selling or sharing personal information about consumers.

The bill further includes within the definition of a covered business (1) the franchisees or franchisors⁷³ of a business that meets the above qualifications, and (2) all of the entities involved in a joint venture or partnership, if the business has at least a 40 percent interest therein. To prevent the improper sharing of personal information between businesses, the bill prohibits each business within the joint venture or partnership from sharing a consumer's personal information with its partner business using the common entity (joint venture or partnership) as a pass through. The businesses are permitted to share a consumer's personal information with the joint venture or partnership, however.

The bill specifically excludes from the definition of a joint venture any third party that operates, hosts, or manages a website or an online service on behalf of a business or processes information on behalf of a business.

Service Providers

A service provider is a person in an express contractual relationship with a business for which it processes personal information that it receives from the business. The contract between the parties must prohibit the service provider from:

- Selling the information;
- Retaining, using or disclosing the personal information it receives from the business for any reason other than that specified in the contract;
- Combining personal information it receives from or on behalf of the business with any other business, or that it collects on its own; and
- Retaining, using, or disclosing personal information outside of the direct business relationship created by the contract.

A business that collects and sells consumer personal information may disclose consumer personal information to a service provider without notice to or consent from the consumer. However, this disclosure must be made pursuant to a contract between the disclosing business and the service provider that prohibits the sale, retention, use, or disclosure of the personal information for any purpose other than the service specified in the contract. The contract must also require that the service provider does not combine a consumer's personal information it receives from multiple businesses or from its own interactions with the consumer.

If a service provider discloses personal information in violation of such a contract, the business generally cannot be found liable. Conversely, a service provider is not liable for duties and obligations assigned to a business under the Act.

Third Parties

A third party is any person who is neither a business that collects person information from a consumer during an intentional interaction with him or her, nor the business' service provider.

⁷³ A franchisee or franchisor is "an entity that controls or is controlled by a business and that shares common branding with the business." Control, for purposes in the bill, means the ownership of, or power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business or the control in any manner over the election of a majority of the directors or individuals who exercise similar functions, or the power to exercise a controlling influence over the management of a company.

A business may sell collected personal information to a third party, but similar to a business' disclosure to a service provider; this sale must be based on a contract that expressly obligates the third party to comply with applicable provisions of the Act—especially regarding the provision of privacy protection.

A service provider may also engage a third party to assist with its performance under a contract for processing personal information, but it must also create a contract with the third party, which shows the third party's understanding and ability to comply with the privacy and security obligations of the Act.

General Business Obligations

Generally, a business may use consumer personal information for a business purpose, which is the business' or service providers' operational purposes. The term "business purpose" may also encompass any reason for which a business gives proper consumer notice (however, service providers are not granted this leeway). The bill provides a non-exhaustive list of permitted business purposes, which includes:

- Auditing related to determining the effectiveness of an advertisement;
- Ensuring the security and integrity of a network or information system, confidentiality of personal information, and physical safety of natural persons;
- Debugging to identify and repair errors that impair functionality;
- Short-term, transient use such as for nonpersonalized advertising –if it does not involve disclosure of personal information or profiling of the consumer;
- Performing services on behalf of the business such as fulfilling orders, processing payments, providing financing, and providing customer service;
- Providing advertising and marketing services that exclude targeted advertising, with specific limits on the combination of personal information;
- Undertaking internal research for technological development and demonstration; and
- Undertaking activities to verify or maintain the quality or safety of a service or device, and to provide upgrades for any such service or device.

Any business' collection, use, retention, and sharing of personal information must be reasonably necessary to achieve, and proportionate to the benefit of achieving, the business purpose.

Notice of Collection of Personal Information

Covered businesses that collect or control the collection of consumer personal information must make the following information reasonably accessible to those consumers from whom they collect personal information through their website or online service:

- The categories of personal information that they collect through their websites or online services, and the categories of third parties with whom they share this information;
- The process, if applicable, through which a consumer may review and request changes to the personal information collected about him or her through the website or online service;
- Whether the business allows a third party to collect the consumer's personal information mined from their online activities over time and across different websites or online services when the consumer uses the business' website or online service; and

- The notice’s effective date and how the business will notify a consumer of material changes to the notice.

This notice must be “reasonably accessible.” It does not appear that this requires a business to post the notice online.

A similar notice is required for a business that controls the collection of consumer personal information that will be used for a non-business purpose, which must inform its consumers of each category of personal information it collects or uses and why it collects or uses that information. The business cannot collect or use types of personal information outside of this notice without first updating the notice to reflect a new category and purpose.

Notice of Retention of Personal Information

Covered businesses are not required to retain consumer personal information, but if they do, they must do so only for as long as is reasonably necessary to effectuate the purpose for which they collected it. However, a covered business can retain de-identified or aggregate consumer information for any amount of time.

A business that collects a consumer’s information for a non-business purpose must inform the consumer from whom it collects that it will retain his or her information. This notification must include the length of time the business expects to retain the information; if the business does not know the duration—it must provide the criteria it will use to determine it.

Notice of Consumer Rights

As discussed above, the bill grants consumers specific rights regarding their personal information. A business that sells a consumer’s information must post a notice to consumers that (1) their information may be sold, and (2) they have the right to opt out of such a sale. This notice requirement may not apply to all covered businesses, as the sale of personal information is required to trigger this notice requirement. Additionally, it is unclear what method of notice is required.

Additionally, specific businesses⁷⁴ must post a clear and conspicuous link with the specific title “Do Not Sell My Personal Information” on their homepages to enable the consumer or an authorized actor to opt out of the sale of the consumer’s personal information. Alternately, a covered business may maintain a separate and additional home page that is dedicated to providing Florida consumers with the required privacy information, if it takes reasonable steps to direct Florida consumers to that specialized webpage.

Employee Education

The bill requires covered business to educate their employees who handle consumer inquiries about the business’ privacy practices and compliance about the bill’s requirements and how to counsel consumers to exercise their rights granted under the bill.

⁷⁴ This requirement applies to “a business that is required to comply with this section.” There is no explicit statement of what types of businesses must comply with s. 501.175, “Use of personal information; third parties; other rights” within the bill.

Data Security

A business that collects a consumer's personal information must implement reasonable security procedures and practices to protect the information from unauthorized or illegal access, destruction, use, modification, or disclosure. This will apply to a large portion of businesses subject to the bill, as even those that keep collected personal information entirely within their business will be required to implement security protections to comply with this provision.

Exclusions

Section 6 of the bill provides specific exclusions or exemptions from the bill.

The bill does not govern the sale, use, retention, or disclosure of de-identified personal information or aggregate consumer information from which individual consumer identities have been removed. Additionally, it permits the sale of personal information if every aspect of that conduct takes place outside of Florida; the consumer's information must have been collected while he or she was not in Florida, and no part of the resulting sale may have occurred in Florida.

The bill expressly allows covered business to do the following:

- Comply with federal, state, or local laws;
- Comply with civil, criminal, or regulatory inquiry or an investigation, a subpoena, or a federal, state, or local summons;
- Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law; and
- Exercise or defend legal claims.

The bill also states that those rights afforded and obligations imposed may not adversely affect the rights and freedoms of other consumers.

The bill provides express exemptions for the following types of information:

- Personal information collected or disclosed by a business in the scope of its role as an employer regarding its employees, applicants, interns, or volunteers;
- Health information collected by a covered entity or its businesses associate as governed by HIPPA and its associated rules;
- Information collected as part of a clinical trial that is subject to the Federal Policy for the Protection of Human Subjects pursuant to specific industry guidelines;
- Personal information that is sold to or by a consumer reporting agency, for use in or to generate a consumer report and limited by the Fair Credit Reporting Act;
- Personal information collected, processed, sold, or disclosed pursuant to GLBA and its implementing regulations;
- Personal information collected, processed, sold, or disclosed pursuant to DPPP;
- Education information covered by FERPA;
- Personal information that is collected, processed, sold, or disclosed relating to the price, route, or service by entities that are subject to the federal Airline Deregulation Act, and only to the extent that this Act is preempted by s. 41713 of the federal Airline Deregulation Act; and

- Vehicle Information or ownership information that is retained by or shared between a new motor vehicle dealer and the vehicle's manufacture, if done so to effectuate a warrantied vehicle repair or recall.

Enforcement

Section 7 grants affected consumers a private right of action against a business for its violation of the Act. Specifically, a consumer may bring a civil action for recovery of:

- Damages of between \$100-\$749 per consumer, per incident or actual damages—whichever is greater;
- Injunctive or declaratory relief;
- Reasonable costs of enforcement, including a reasonable attorney fee; and
- Any other relief a court deems proper.

The bill separately grants the Department of Legal Affairs authority to bring an action against a business it has reason to believe is violating or has violated the Act. The trial court may issue a temporary or permanent injunction, impose a civil penalty of \$5,000 or less per violation (this may be tripled if the consumer was under 16 years of age at the time of the violation), award reasonable enforcement costs—including a reasonable attorney fee, and grant any other relief it deems appropriate.

The bill grants the Department of Legal Affairs rulemaking authority to enforce the Act.

Effective Date

Section 8 of the bill provides that the Act will take effect on January 1, 2022.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

Any public records or open meetings issues are addressed in SB 7064 (2021 Regular Session).

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None.

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 similar privacy practices based on legislation in California, Illinois, and the E.U.

C. Government Sector Impact:

The DLA will likely see an increase in prosecutions and other regulatory activity relating to the Act. Additionally, the Judiciary may see an increase in caseload as a result of private actions filed under the Act.

VI. Technical Deficiencies:

The bill requires service providers that disclose personal information with a third party in furtherance of their contractual duties to do so pursuant to a contract that outlines the third party's duty to maintain the security of the shared personal information. The bill describes this duty as "that described in s. 501.174(23)," but this section does not include a duty—it only defines "security and integrity." This provision may be more clear if it replaces the reference to s. 501.174(23) with a reference to s. 501.1745(3), F.S., which requires businesses that collect consumer personal information to implement reasonable security procedures and practices.

Section 501.175, as created by the bill, generally creates business duties to notify consumers of rights regarding their personal information. Most subsections of the bill apply to "a business that sells consumers' personal information," but subsection (5) refers to "a business that is required to comply with this section." There is no general statement of applicability within s. 501.175, and therefore it may be unclear to which businesses these duties created by s. 501.175(5), F.S., apply.

The committee substitute adds geolocation data as information that is considered personal information. This is repetitive, as personal information was already defined to include "audio, electronic, visual, thermal, olfactory, *geolocation*, or similar information."

VII. Related Issues:

The bill grants the DLA rulemaking authority to enforce the Act and otherwise permits it to institute appropriate legal proceedings where it believes necessary. However, the DLA may require investigative authority. For example, s. 501.206, F.S., grants the DLA authority to administer oaths and affirmations, subpoena witnesses or matter, and collect evidence in furtherance of its enforcement authority under the Florida Deceptive and Unfair Trade Practices Act.

The bill appears to provide inconsistent guidance regarding re-authorization of the consumer's opt out request. For example, the bill states that once a consumer opts out, the business must comply without requiring any additional consumer action if it can identify the consumer through a login protocol or a user-enabled global privacy control. The bill states elsewhere that a business that received an opt-out request cannot sell the consumer's personal information until it receives the consumer's subsequent express authorization. Section 501.175(5)(d) of the bill also permits a business to request a consumer to re-authorize his or her opt-out after 12 months have passed from initial receipt of the consumer's preference.

VIII. Statutes Affected:

This bill creates the following sections of the Florida Statutes: 501.172, 501.173, 501.174, 501.175, 501.176, 501.177.

IX. Additional Information:**A. Committee Substitute – Statement of Substantial Changes:**
(Summarizing differences between the Committee Substitute and the prior version of the bill.)**CS by Commerce and Tourism on March 22, 2021:**

- Re-defines the term “consumer” so that an individual is no longer required to seek or acquire a good or service from a business to accrue the rights granted by the bill;
- Clarifies that information a consumer shares with the public, or truthful information that concerns a public matter, is not personal information regulated by the bill;
- Broadens the definition of a “business purpose” to include any reason for which a business gives proper notice to its consumers, thereby creating a more a flexible business purpose;
- Instills a corresponding business duty to provide an accounting of personal information it collects about an individual consumer upon his or her request;
- Clarifies that a business is required to provide requesting consumers an accounting of the personal information the business collected on or after July 1, 2022.
- Implements a requirement that covered businesses inform consumers of the duration they intend to retain personal information, and require that the retention be for no longer than reasonably necessary to accomplish the business purpose for which it was collected;
- Requires a covered business to comply with a consumer's opt-out request within 2 days, versus 15;

- Requires a covered business to implement data security measures to protect consumer personal information;
- Excludes specific information from the act, including information subject to enumerated federal privacy regulations, information collected or disclosed by an employer about its employees in the regular scope of its duties, and information held or shared by a car dealer and manufacturer for car repairs, recalls, and maintenance; and
- Delays the effective date to January 1, 2022.

B. Amendments:

None.