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 1734
INTRODUCER:	Senator Bradley
SUBJECT:	Consumer Data Privacy
DATE:	March 19, 2021
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Harmsen	McKay	CM	**Pre-meeting**
2.			AP	
3.			RC	

I. Summary:

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;
- 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.

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 July 1, 2021.

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 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]

---

[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. 19, 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. 19, 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. 19, 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. 19, 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. 19, 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. 19, 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. 19, 2021).

[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. 19, 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. 19, 2021).

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 entities[14] 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;
  - 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:

---

[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. 19, 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. 19, 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. 19, 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. 19, 2021). Section 501.171(3)-(4), F.S.
[16] Section 501.171(3)-(6), F.S.
[17] Section 501.171(1)(g)1., F.S.; OAG *supra* note 15.

- 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 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]

---

[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. 19, 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. 19, 2021).
[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

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 (HIPPA)[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 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 impressible uses or disclosures; and

[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. 19, 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. 19, 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.
[29] 45 C.F.R. §164.302-318.

- 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.

Fair Credit Reporting Act (FCRA)[30]

The FCRA promotes the accuracy, fairness, and privacy of information that consumer reporting agencies and their related entities collect.[31] 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.[32]

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.[33]

Children's Online Privacy Protection Act (COPPA)[34]

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;

[30] 15 U.S.C. §1681.
[31] 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. 19, 2021). *See also*, Federal Trade Commission, *Fair Credit Reporting Act*, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited Mar. 19, 2021).
[32] 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).
[33] 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).
[34] 16 C.F.R. pt. 312.

- 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.[35]

COPPA further requires covered entities to:[36]

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

Violations of COPPA are 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.[37]

Driver's Privacy Protection Act (DPPA)[38]

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.

[35] 15 U.S.C. §§ 6502(a)-(b).
[36] *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. 19, 2021).
[37] 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. 19, 2021).
[38] 18 U.S.C. §2721.

Violations of the DPPA are subject to criminal fine. Additionally, a private individual affected by the improper disclosure or use of his or her personal information may bring a private civil action against the violator.[39]

Family Educational Rights and Privacy Act (FERPA)[40]

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.[41]

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.[42] 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.[43]

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.[44]

The FTC generally cannot seek civil penalties for violations of the FTC Act, but may asses civil monetary penalties for repeated offenses.[45] There is no private right of action granted under the FTC Act.

---

[39] 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. 19, 2021).
[40] 20 U.S.C. §1232(g); 34 C.F.R. § 99.
[41] 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. 19, 2021).
[42] 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. 19, 2021).
[43] 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. 19, 2021).
[44] *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. 19, 2021). (last visited Mar. 19, 2021); and Complaint In the Matter of Sears Holdings Mgmt Co., No. C-4264 (F.T.C. Aug. 31, 2009).
[45] 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. 19, 2021).

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).[46] 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.[47]

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.[48] 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.[49]

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.[50] This report must be provided to the individual within one month of his or her request.[51] 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.

---

[46] *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. 19, 2021).
[47] GDPR, art. 3.
[48] 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. 19, 2021).
[49] 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. 19, 2021).
[50] 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. 19, 2021).
[51] GDPR, arts. 12(3), 15.

Under BIPA, a private entity:[52]

- 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.
- 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.[53]

On January 25, 2019, 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.[54] 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.[55]

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.[56] 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.

[52] 740 Ill. Comp. Stat. 14/10, 14/15 (2008).
[53] 740 Ill. Comp. Stat. 14/20 (2008).
[54] *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.
[55] *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).
[56] Cal. Civ. Code § 1798.140(O)(1).

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 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.[57]

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.[58] 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.[59]

---

[57] 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. 19, 2021).
[58] Va. Code Ann. § 59.1-573 (2020).
[59] Va. Code Ann. § 59.1-571 (2020).

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.[60]

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.[61] 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.[62]

The Virginia Attorney General has exclusive enforcement authority of the Virginia Act.[63]

	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	DPAs
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

[64]

[60] Va. Code Ann. § 59.1-572 A (2020).
[61] Va. Code Ann. § 59.1-572 B (2020).
[62] Va. Code Ann. § 59.1-572 C (2020).
[63] *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. 19, 2021).
[64] 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. 19, 2021).

III. Effect of Proposed Changes:

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 and process personal information about consumers.

Consumer Rights

The bill defines a consumer as a person who seeks or acquires any good, service, money, or credit from a business while he or she is either in Florida for a purpose that is not temporary or transitory, or is temporarily or transitorily outside of the state—but is domiciled in Florida. The term specifically excludes nonresidents.

Personal Information

The bill defines personal information as specific information about a consumer or household that a covered business collected and maintains in an accessible format.

More specifically, personal information is 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 that allows one to contact the consumer in-person or online;
- Biometric information,[65] 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, his or her browsing history, search history, and information regarding a consumer's interaction with a website, an application, or an 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; or
- Information that may serve as a probabilistic identifier[66] concerning him or her which is collected from the consumer through a website, an online service, or some other means by the business and maintained by the business in combination with an identifier in a form that, when used together with the information, identifies the consumer.

[65] The bill further 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."

[66] The bill further 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.

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;
- 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; and
- Information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act and any regulations adopted pursuant thereto.

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.

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 opted-in. This does not prevent businesses from collecting the individual personal information from 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 be subject to penalty under the bill if it fails to institute some method to determine its consumer's 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 or older to instruct a business that sells personal information not to sell his or her personal information. As discussed below,[67] "sale" is defined expansively by the bill to include any transfer or communication of consumer personal data to advance a business' economic interests.

[67] *See infra*, Notice Requirements: Notice of Sale of Personal Information.

The business must stop selling the consumer's personal information within 15 days after it receives an opt-out request. The business may not require a consumer to create an account to submit his or her opt out request. Additionally, the business cannot require a consumer to declare his or her privacy preferences at each encounter with a business' website.

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.

Targeted Advertisements

The right to opt-out includes a right to opt-out of specific data profiling and targeted advertising.

"Profiling that produces legal or similarly significant effects concerning the consumer" is defined as the "automatic processing that a business performs on his or her 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 nonaffiliated websites or applications. As defined by the bill, targeted advertising does not include advertisements based on a consumer's (1) activity within the website or application, (2) current search query or visit to a website or application, and (3) request for information or feedback. The term's definition also excludes data processed with the exclusive purpose of measuring or reporting advertising performance, reach, or frequency.

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.

Duration of opt out

Once a consumer instructs a business that it may not to sell his or her personal information, the business is prohibited from doing so until it receives the consumer's subsequent express authorization. The bill further instructs that a business cannot require a consumer to take additional actions to renew their opt-out request if it is able to identify the consumer through a login protocol, 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.

However, section 501.175(4)(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. This may be inconsistent with the provision that requires a consumer's express re-authorization of the use of his or her personal information.

Non-Discrimination

A consumer who opts out of the sale of his or her personal information is guaranteed the right to receive equal service and pricing from covered businesses. Specifically, if a consumer opts-out of the sale of his or her personal information, the covered business cannot deny him or her goods or services, charge a different price, or provide a different quality of goods or services.

A consumer who opts-out of the general sale of his or her personal information is more protected from discriminatory business behavior than a consumer who opts-out of targeted advertising practices.[68]

Verified Requests

A consumer must make a verified request to exercise their rights to 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 request to exercise their rights under the bill; the address may be either an e-mail address, toll-free phone number, or website through which a consumer may submit a verified request. 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 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

[68] *See supra*, Targeted Advertisements.

consumer of the underlying reason. It is the business' burden to demonstrate that the consumer's verified request was unfounded or burdensome.

Right to Delete Personal Information

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

A consumer's request to delete his or her personal information 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.

Where a business has already de-identified the personal information, it cannot be required to re-identify 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 consumer must make this request, and cannot authorize a third party to do so on his or her behalf.

Right to Submit a Verified Request for Information Regarding the Manner of Public Information Collected

The bill requires a business to ensure that consumers have a right to submit a verified request to discover the sources from which a business collects his or her personal information, the specific elements of personal information collected, and to whom the business sold the consumer's personal information. However, this right to request does not appear to be paired with a right to receive the information in a manner that is specific to the consumer. However, covered businesses are required to make this information, in a general manner (as applicable to all of its users), reasonably accessible to its consumers.[69]

Business Requirements

Covered Businesses

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

[69] *See infra*, Notice of Collection of Personal Information.

- 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 franchisors[70] 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 covered business 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; or an entity that is subject to the Health Insurance Portability and Accountability Act (HIPPA) of 1996[71] and the regulations adopted pursuant thereto.

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 itself. The contract between the parties must prohibit the service provider from (1) using or disclosing the personal information it receives from the business for any reason other than that specified in the contract, and (2) combining personal information it receives from the business with any other business, or that it collects on its own.

A business 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 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 cannot generally be found liable.

[70] 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.
[71] Pub. L. No. 104-191.

Notice Requirements

Notice of Sale of Personal Information

The bill requires businesses that sell consumers' personal information to third parties to provide 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.

The definition of "sale" in the bill is expansive, however, and includes any of the following activity between businesses if done for monetary, tangible or intangible consideration, or for any other purpose that would advance a business' economic interests: selling, renting, releasing, disclosing, disseminating, making available, loaning, sharing, transferring, or otherwise communicating a consumer's personal information. The following business activity is not considered a sale under the bill: a business' disclosure to (1) a service provider that processes the personal information on behalf of the business or (2) to another business with which the consumer has a direct relationship, to provide a product or service that the consumer requested. This permits a business to, e.g., transfer a consumer's address to the U.S. Post Office to facilitate the mailing of an ordered item.

Covered businesses must also 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.

Notice of Collection of Personal Information

Covered businesses that collect 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 a business must post the notice online.

Education of Employees

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.

Exclusions

Section 5 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 approaches information that is otherwise regulated by Federal privacy laws in various manners. For example, the bill excludes entities subject to HIPPA from the definition of a business under the Act, and therefore excludes those entities from the requirements of the Act. Whereas, the Act expressly exempts the sale of personal information to or from a consumer reporting agency if the information will be reported in or used to generate a consumer report as defined under the FCRA from its auspices entirely. Information collected, processed, sold, or disclosed by a financial institution pursuant to the GLBA and its regulations is excluded from the definition of personal information, "if it is inconsistent with that act, and only to the extent of the inconsistency."

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.

Enforcement

Section 6 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.

Effective Date

Section 7 of the bill provides that the Act will take effect on July 1, 2021.

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:

The bill requires a business to request that a third party delete a consumer's personal information if the business shared such information with the third party and subsequently received a request to delete it. This requirement may impair performance under the contract if the personal information was shared by the business pursuant to a contract.

The United States Constitution and the Florida Constitution prohibit the state from passing any law impairing the obligation of contracts.[72] "[T]he first inquiry must be whether the state law has, in fact, operated as a substantial impairment of a contractual relationship. The severity of the impairment measures the height of the hurdle the state legislation must clear."[73] If a law does impair contracts, the courts will assess whether the law is deemed reasonable and necessary to serve an important public purpose.[74] The

[72] U.S. Const. Article I, s. 10; Art. I, s. 10, Fla. Const.
[73] *Pomponio v Claridge of Pompano Condominium, Inc.*, 378 So. 2d 774, 779 (Fla. 1979) (quoting *Allied Structural Steel Co. v. Spannaus*, 438 U.S. 234, 244-45 (1978)). *See also General Motors Corp. v. Romein*, 503 U.S. 181 (1992).
[74] *Park Benziger & Co. v. Southern Wine & Spirits, Inc.*, 391 So. 2d 681, 683 (Fla. 1980); *Yellow Cab Co. of Dade County v. Dade County*, 412 So. 2d 395, 397 (Fla. 3rd DCA 1982) (citing *United States Trust Co. v. New Jersey*, 431 U.S. 1 (1977)).

factors that a court will consider when balancing the impairment of contracts with the public purpose include:

- Whether the law was enacted to deal with a broad, generalized economic or social problem;
- Whether the law operates in an area that was already subject to state regulation at the time the parties undertook their contractual obligations, or whether it invades an area never before subject to regulation; and
- Whether the law results in a temporary alteration of the contractual relationships of those within its scope, or whether it permanently and immediately changes those contractual relationships, irrevocably and retroactively.[75]

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:

It appears that the bill has conflicting guidance regarding the duration of a consumer's choice to opt-out.

Section 501.177, created by section 6 of the bill, grants the DLA authority to institute legal proceedings against businesses that have violated "this section." This should refer to "any provision of the Act" instead, as there is no violation outlined in section 501.177, F.S.

The bill excludes from the definition of personal information "[i]nformation collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq., and regulations adopted pursuant thereto, if it is inconsistent with that act, and only to the

[75] *See supra* note 74.

extent of the inconsistency." The language regarding inconsistency may need to be amended for clarity.

VII. Related Issues:

None.

VIII. Statutes Affected:

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

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.