HOUSE OF REPRESENTATIVES STAFF FINAL BILL ANALYSIS

BILL #: CS/HB 1547 Technology Transparency
SPONSOR(S): Regulatory Reform & Economic Development Subcommittee, McFarland and others
TIED BILLS: CS/HB 1549 **IDEN./SIM. BILLS:** CS/CS/SB 262

FINAL HOUSE FLOOR ACTION: 110 **Y's** 2 **N's** **GOVERNOR'S ACTION:** Approved

SUMMARY ANALYSIS

CS/HB 1547 passed the House on May 3, 2023, as CS/CS/SB 262, as amended. The bill was amended in the Senate on May 4, 2023, and returned to the House. The House concurred in the Senate amendments, and subsequently passed the bill as amended on May 4, 2023.

Due to the growth in businesses that collect personal information for the purpose of selling targeted advertising on the Internet, many countries and states have adopted or updated laws relating to the collection and use of personal information. Specifically, the European Union, and states like California, Virginia, and Illinois, have enacted data privacy laws to protect consumers' personal information.

The bill requires certain businesses with over $1 billion in gross annual revenues to publish a privacy policy for personal data, and defines "personal data" as any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual, including pseudonymous data when used with information linking the data to an identified or identifiable individual. The term does not include certain public information, employee information, or deidentified or aggregate information.

The bill gives consumers rights related to personal data collected by certain businesses with over $1 billion in gross annual revenues, including:

- The right to access personal data collected;
- The right to delete or correct personal data; and
- The right to opt-out of the sale of personal data.
- The right to opt-out of processing of sensitive data or geolocation.

The bill provides that online platforms predominantly accessed by children under 18 years of age may not, except under certain situations:

- Process personal information of or profile a child.
- Collect, sell, share, or retain personal information or geolocation of a child.
- Use a child's personal information for any unstated reason.
- Use dark patterns to obtain more information of a child than necessary.
- Use collected information to estimate age for any other reason.

The bill allows the Department of Legal Affairs (DLA) to enforce such rights by bringing an action against, and collecting civil penalties from, online platforms or businesses that violate a consumer's rights as provided in the bill.

The bill also adds "biometric data" and "geolocation" to the definition of "personal information" under the Florida Information Protection Act (FIPA). As such, entities in possession of such information must take reasonable measures to protect biometric and geolocation data and report data breaches.

The bill provides that certain government employees may not request that a social media platform remove content or accounts from social media platforms and prohibits a governmental entity from working with a social media platform for the purpose of content moderation, with certain exceptions including routine account management of the government entity's account.

The bill has no fiscal impact on local governments, and an indeterminate fiscal impact on state government.

The bill was approved by the Governor on June 6, 2023, ch. 2023-201, L.O.F., and will become effective on July 1, 2024.

I. SUBSTANTIVE INFORMATION

A. EFFECT OF CHANGES:

Consumer Data Privacy – Current Situation

Florida Deceptive and Unfair Trade Practices Act (FDUTPA)

FDUTPA is a consumer and business protection measure that prohibits unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in trade or commerce.[1] FDUTPA was modeled after the Federal Trade Commission (FTC) Act.[2]

The DLA or the Office of the State Attorney (SAO) may bring actions on behalf of consumers or governmental entities when it is a matter of public interest.[3] The SAO may enforce violations of FDUTPA if the violations take place within its jurisdiction. The DLA has enforcement authority when the violation is multi-jurisdictional, the state attorney defers to the DLA in writing, or the state attorney fails to act within 90 days after a written complaint is filed.[4] In certain circumstances, consumers may also file suit through private actions.[5]

The DLA and the SAO have powers to investigate FDUTPA claims, which include:[6]

- Administering oaths and affirmations;
- Subpoenaing witnesses or matter; and
- Collecting evidence.

The DLA and the State Attorney, as enforcing authorities, may seek the following remedies:

- Declaratory judgments;
- Injunctive relief;
- Actual damages on behalf of consumers and businesses;
- Cease and desist orders; and
- Civil penalties of up to $10,000 per willful violation.[7]

FDUTPA may not be applied to certain entities in certain circumstances, including:[8]

- Any person or activity regulated under laws administered by the Office of Insurance Regulation or the Department of Financial Services; or
- Banks, credit unions, and savings and loan associations regulated by the Office of Financial Regulation or federal agencies.

Consumer Data

---

[1] Ch. 73-124, L.O.F.; s. 501.202, F.S.
[2] D. Matthew Allen, et. al., *The Federal Character of Florida's Deceptive and Unfair Trade Practices Act*, 65 U. MIAMI L. REV. 1083 (Summer 2011).
[3] S. 501.207(1)(c) and (2), F.S.; *see* s. 501.203(2), F.S. (defining "enforcing authority" and referring to the office of the state attorney if a violation occurs in or affects the judicial circuit under the office's jurisdiction; or the Department of Legal Affairs if the violation occurs in more than one circuit; or if the office of the state attorney defers to the department in writing; or fails to act within a specified period); *see also* David J. Federbush, *FDUTPA for Civil Antitrust: Additional Conduct, Party, and Geographic Coverage; State Actions for Consumer Restitution*, 76 FLORIDA BAR JOURNAL 52, Dec. 2002 (analyzing the merits of FDUPTA and the potential for deterrence of anticompetitive conduct in Florida), *available at* http://www.floridabar.org/divcom/jn/jnjournal01.nsf/c0d731e03de9828d852574580042ae7a/99aa165b7d8ac8a485256c8300791ec1!OpenDocument&Highlight=0,business,Division* (last visited on Mar. 25, 2023).
[4] S. 501.203(2), F.S.
[5] S. 501.211, F.S.
[6] S. 501.206(1), F.S.
[7] Ss. 501.207(1), 501.208, and 501.2075, F.S. Civil Penalties are deposited into general revenue. Enforcing authorities may also request attorney fees and costs of investigation or litigation. S. 501.2105, F.S.
[8] S. 501.212(4), F.S.

As technologies that capture and analyze data proliferate so do businesses' abilities to contextualize consumer data. Businesses use such data for a range of purposes, including better understanding day-to-day operations to increase revenue, making informed business decisions, learning about their customer base, and tailoring marketing strategies.[9]

From consumer behavior to predictive analytics, companies regularly capture, store, and analyze large amounts of quantitative and qualitative data on their consumer base. Some companies have built an entire business model around consumer data, which may include the company are selling personal information to a third party or creating targeted ads for specific consumers.[10]

Generally, the types of consumer data that businesses collect are:[11]

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

General Data Protection Regulation (European Union)

In 2016, The European Union passed a broad data privacy law that addressed several areas of consumer rights and data protection called the General Data Protection Regulation (GDPR).[12] The law became effective in 2018 and unified the regulatory approach to data privacy across the European Union. The GDPR has since become a model for other data privacy laws in other countries, including Chile, Japan, Brazil, South Korea, Argentina, and Kenya.[13]

Under the GDPR, personal data includes anything that allows a person to be identified. Individuals, organizations, and companies that are either "controllers" or "processors" of personal data are covered by the law. Controllers exercise overall control of the purposes and means of processing personal data; whereas processors act on behalf of, and only on the instructions of, the relevant controller.[14]

Before processing or collecting any personal data, a business must explicitly request permission from the subject or person to do so. The request must use clear language and is commonly referred to as a data "opt-in."

The GDPR specifically bans the use of lengthy documents filled with legalese to confuse or frustrate the consumer. Hiding permissions to collect and use data within a contract's Terms and Conditions or Privacy Policy sections is not permissible under the GDPR. Consent must be given for a specific purpose and must be requested separately from other documents and policy statements. [15]

---

[9] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Jun. 17, 2020) https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (last visited Mar. 25, 2023).
[10] *Id*.
[11] *Id*.
[12] European Data Protection Supervisor, *The History of the General Data Protection Regulation*, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Mar. 25, 2023).
[13] *Id*.
[14] Wired, *What is the GDPR? The Summary Guide to GDPR Compliance in the UK*, https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (last visited Mar. 25, 2023).
[15] TechRepublic, *GDPR: A Cheat Sheet*, https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/ (last visited Mar. 25, 2023).

The GDPR requires companies to provide, at the data subject's request, confirmation as to whether personal data pertaining to them is being processed, where it is being processed, and for what purpose. A company must also provide, free of charge**,** a copy of the personal data being processed in an electronic format to the consumer.[16]

Under the GDPR, a company must erase all personal data when asked to do so by the subject consumer. At that point, the company must cease further dissemination of the data and halt all processing of that consumer's data. Valid conditions for erasure include situations where the data is no longer relevant, the original purpose has been satisfied, or a subject consumer withdraws consent.[17]

The GDPR requires a company to provide mechanisms for a subject to receive any previously provided personal data in a commonly used and machine-readable format.[18]

The GDPR allows private rights of action for violations of privacy rights; however, the consumer must prove any damages in order to receive compensation.[19]

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

The California Consumer Privacy Act of 2018 (CCPA) was passed to give consumers more control over the personal information that businesses collect. This landmark law granted new privacy rights for California consumers, including:[20]

- The right to know about the personal information a business collects, specifically about the consumer, and how it is used and shared;
- The right to delete personal information collected with some exceptions;
- The right to opt-out of the sale of personal information; and
- The right to non-discrimination for exercising the CCPA rights.

The CCPA applies to for-profit businesses that do business in California that also meet any of the following:[21]

- 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.

Businesses must give consumers certain notices explaining their privacy practices and provide certain mechanisms to allow consumers to exercise their rights.[22]

The law is largely enforced by the Attorney General, and businesses are subject to fines for violating the law. A consumer may only bring a cause of action against a business if certain categories of personal information tied to his or her name have been stolen in a nonencrypted and nonredacted form.[23] As of July 2020, approximately 50 suits had been filed pursuant to this provision.[24]

The California Privacy Rights Act (CPRA) passed in 2020 as a statewide proposition, though it is not effective until January 1, 2023. The CPRA amends and expands the CCPA. Specifically dealing with

---

[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] Art. 82 of the GDPR.
[20] State of California Department of Justice, Office of the Attorney General, California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa (last visited Mar. 25, 2023).
[21] Cal. Civ. Code s. 1798.140.
[22] Cal. Civ. Code ss. 1798.130, 1798.135.
[23] Cal. Civ. Code ss. 1798.150, 1798.155.
[24] Holland & Knight LLP, *Litigating the CCPA in Court*, Litigating the CCPA in Court | Insights | Holland & Knight (hklaw.com) (last visited Mar. 25, 2023).

certain areas of concern with the CCPA, the CPRA created a new agency to handle complaints and enforcement. The CPRA changes the CCPA by:[25]

- Allowing a consumer to:
  - Prevent businesses from sharing his or her personal information;
  - Correct inaccurate personal information; and
  - Limit businesses' use of "sensitive personal information"—including precise geolocation; race; ethnicity; religion; genetic data; private communications; sexual orientation; and specified health information;
- Establishing California Privacy Protection Agency to additionally enforce and implement consumer privacy laws and impose fines;
- Changing criteria for which businesses must comply with laws by:
  - Doubling the CCPA's threshold number of consumers or households from 50,000 to 100,000, resulting in reduced applicability of the law to small and midsize businesses;
  - Expanding applicability to businesses that generate most of their revenue from sharing personal information, not merely selling it; and
  - Extending the definition to joint ventures or partnerships composed of businesses that each have at least a 40 percent interest.
- Prohibiting businesses' retention of personal information for longer than reasonably necessary;
- Tripling maximum penalties for violations concerning consumers under age 16; and
- Authorizing civil penalties for theft of consumer login information.

California Age-Appropriate Design Code Act

In 2022, California adopted the California Age-Appropriate Design Code Act (CAADCA), an amendment to the CPRA,[26] legislation modelled on the United Kingdom's Age Appropriate Design Code,[27] which requires online platforms to adhere to strict default privacy and safety settings that protect the best interest of children.[28] CAADCA covers children under 18 years of age and will be effective July 1, 2024.[29]

CAADCA requires certain businesses that provide an online service, product, or feature that is likely to be accessed by children to comply with several new requirements and restrictions, including:[30]

- Prohibitions on using any personal information that it knows or should know is materially detrimental to a child's physical or mental health and/or wellbeing; and
- Prohibitions on obscuring user interface features to deliberately defeat consent or manipulate children into providing unnecessary personal information, otherwise called "dark patterns."

Such businesses must complete a Data Protection Impact Assessment for any new feature they wish to offer to the public if it is likely to be accessed by children, which will determine if any dark patterns are employed, if there is an asymmetrical reward, or if targeted advertisements are deployed in a way that could harm or exploit children.[31]

Virginia Consumer Data Protection Act

---

[25] Ballotpedia, *California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*, https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020) (last visited Mar. 25, 2023).
[26] Cal. Civil Code § 1798.99.28-.35
[27] 5Rights Foundation, *California follows UK lead as child data protection law is passed*, https://5rightsfoundation.com/in-action/california-follows-uk-lead-as-child-data-protection-law-is-passed.html (last visited Mar. 2, 2023).
[28] Office of Governor Gavin Newsome, *Governor Newsom Signs First-in-Nation Bill Protecting Children's Online Data and Privacy*, https://www.gov.ca.gov/2022/09/15/governor-newsom-signs-first-in-nation-bill-protecting-childrens-online-data-and-privacy/ (last visited Mar. 2, 2023).
[29] Cal. Civil Code § 1798.99.28-.35
[30] Briana Kelly, Nelson Mullins Riley & Scarborough LLP, *State of California Passes Bill to Protect Children Online*, Jan. 26, 2023, https://www.nelsonmullins.com/idea_exchange/alerts/privacy_and_data_security_alert/all/state-of-california-passes-bill-to-protect-children-online (last visited Mar. 2, 2023).
[31] *Id*.

On March 2, 2021, the Virginia Consumer Data Protection Act (VCDPA) was signed into law.[32] The VCDPA, which becomes effective January 1, 2023, borrows from CCPA and GDPR.[33] Some argue that because Virginia was able to benefit from the experience of businesses that have spent the better part of the last five years implementing GDPR or CCPA, the Virginia law may be a lighter implementation task for companies.[34]

Generally, with regard to personal data, the VCDPA grants consumers the right to access, correct, delete, obtain a copy of, and opt-out of the processing of personal data for the purposes of targeted advertising.

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

- Control or process personal data of at least 100,000 consumers; or
- Derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers.[35]

Colorado Privacy Act

The Colorado Privacy Act (CPA)[36] was signed in to law on July 8, 2021, and is effective July 1, 2023. The law also borrows from the GDPR, CCPA, and VDCPA.[37]

Generally, with regard to personal data, the CPA grants a consumer the right to:[38]

- Access data;
- Correct data;
- Delete data; and
- Move data across different services.

Like the CCPA and VCDPA, CPA contains exceptions for certain types of data and information governed by federal law. It provides that the Attorney General has exclusive authority to enforce violations of the law, and does not provide a private cause of action to a consumer. CPA applies to persons conducting business in the state that either:[39]

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

Illinois Biometric Information Privacy Act

In 2008, Illinois adopted the Biometric Information Privacy Act (BIPA), which puts in place safeguards and procedures relating to the retention, collection, disclosure, and destruction of biometric information

---

[32] JDSupra, *Virginia's Consumer Data Protection Act Has assed: What's in It?*, https://www.jdsupra.com/legalnews/virginia-s-consumer-data-protection-act-1577777/ (last visited Mar. 25, 2023).
[33] Sidley Austin LLP, East Coast Meet West Coast: Enter the Virginia Consumer Data Privacy Protection Act, https://www.sidley.com/en/insights/newsupdates/2021/03/east-coast-meets-west-coast-enter-the-virginia-consumer-data-protection-act (last visited Mar. 25, 2023).
[34] *Id*.
[35] Virginia's Legislative Information System, Bill Summary for SB 1392, https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392S (last visited Mar. 25, 2023).
[36] C.R.S. 1-6-1301-1313
[37] The National Law Review, *And Now There are Three…The Colorado Privacy Act*, July 16, 2021, https://www.natlawreview.com/article/and-now-there-are-three-colorado-privacy-act#:~:text=Colorado%20has%20now%20joined%20California,effect%20on%20July%201%2C%202023. (last visited Mar. 25, 2023).
[38] *Id*.
[39] *Id*.

and specifically protects the biometric information of those in the state. It was the first state law in the U.S. to specifically regulate biometrics.

Under BIPA, a private entity:[40]

- In possession of biometric data (defined as retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry) must have a written policy establishing a retention schedule and guidelines for permanently destroying such data;
- May not collect, capture, purchase, receive through trade, or otherwise obtain biometric data unless it informs the subject that the data is being stored and the manner of storage, and receives a written release from the subject;
- May not profit from a person's biometric data;
- May not disseminate a person's biometric data unless the subject consents, is authorized by the subject, or 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:[41]

- Liquidated damages of $1,000 or actual damages, whichever is greater, against a private entity that negligently violates BIPA;
- Liquidated damages of $5,000 or actual damages, whichever is greater, against a private entity that intentionally or recklessly violates BIPA;
- Reasonable attorneys' fees and costs; and
- Other relief, including an injunction, as the court deems appropriate.

Because Illinois granted a private cause of action for violations of BIPA, there have been several lawsuits claiming damages for privacy and use violations, and Illinois courts have upheld the law. 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 the Act.[42] Court documents also tend to support the notion that an individual in Illinois has a valid cause of action if his or her biometric data is taken without consent by a private entity, including out-of-state entities, but it is subject to a finding of fact.[43]

Additional States

Connecticut and Utah recently signed similar bills to Virginia and Colorado into law. There are also 18 other states that are actively considering data privacy bills.[44]

Federal Laws Addressing Data Privacy

While there is no broad federal law addressing data privacy, generally, there are several industry-specific laws that address the need to keep certain data private or protected.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[45] is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed

[40] 740 Ill. Comp. Stat. 14/10, 14/15 (2008).
[41] 740 Ill. Comp. Stat. 14/20 (2008).
[42] *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186.
[43] *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).
[44] IAPP, *US State Privacy Legislation Tracker*, Mar. 17, 2023, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last visited Mar. 25, 2023).
[45] 42 U.S.C. s. 1320.

without the patient's consent or knowledge. The U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule[46] to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.[47]

HIPAA's Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)" from being disclosed without the patient's consent or knowledge.[48]

"Individually identifiable health information" is information, including demographic data, that relates to:[49]

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual.

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act.[50]

The Security Rule applies to the subset of identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form, and is called "electronic protected health information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing. To comply with the Security Rule, all covered entities must do the following:[51]

- Ensure the confidentiality, integrity, and availability of all electronic protected health information;
- Detect and safeguard against anticipated threats to the security of the information;
- Protect against anticipated impermissible uses or disclosures; and
- Certify compliance by their workforce.

"Covered entities" who must abide by the Privacy Rule and the Security Rule are:[52]

- Health plans;
- Healthcare providers;
- Healthcare clearinghouses; and
- Business associates.

Federal Policy for the Protection of Human Subjects

The Federal Policy for the Protection of Human Subjects, or the "Common Rule," is a rule promulgated by the U.S. Food and Drug Administration (FDA).[53] The Common Rule governs the ethical conduct of research involving human subjects. Fifteen federal agencies and departments are party to this rule, which first came into effect in 1981. The Common Rule has not been substantively updated since 1991.[54] Among other requirements, the Common Rule mandates that researchers protect the privacy of subjects and maintain confidentiality of human subject data.[55]

---

[46] 45 C.F.R. ss. 160 and 164.
[47] Centers for Disease Control and Prevention, Health Insurance Portability and Accountability Act of 1996 (HIPAA), https://www.cdc.gov/phlp/publications/topic/hipaa.html (last visited Mar. 25, 2023).
[48] *Id*.
[49] 45 C.F.R. s. 160.103.
[50] 20 U.S.C. s. 1232(g).
[51] CDC, supra note 47.
[52] 45 C.F.R. ss. 160.102, 160.103.
[53] 21 C.F.R. §§ 50, 60.
[54] U.S. Department of Health and Human Services, Federal Policy for the Protection of Human Subjects ('Common Rule'), Federal Policy for the Protection of Human Subjects ('Common Rule') | HHS.gov (last visited Mar. 25, 2023).
[55] The University of Chicago, *University Data Usage Guide, Sensitive Identifiable Human Subject Research Data*, https://dataguide.uchicago.edu/sensitive-identifiable-human-subject-research-data (last visited Mar. 25, 2023).

The FDA is a member of the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, which brings together the regulatory authorities and pharmaceutical industry to develop guidelines for pharmaceutical trials.[56]

The Fair Credit Reporting Act

The Fair Credit Reporting Act[57] (FCRA) protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services. Information in a consumer report cannot be provided to anyone who does not have a purpose specified in the FCRA. Companies that provide information to consumer reporting agencies also have specific legal obligations, including the duty to investigate disputed information. In addition, users of the information for credit, insurance, or employment purposes must notify the consumer when an adverse action is taken on the basis of such reports.[58]

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act[59] requires financial institutions, such as companies that offer consumers financial products or services like loans, financial or investment advice, mortgages, or insurance, to explain their information-sharing practices to their customers and to safeguard sensitive data.[60]

The law requires that financial institutions protect information collected about individuals; it does not apply to information collected in business or commercial activities.

In certain situations, consumers of a financial institution have opt-out rights from having their nonpublic personal information shared with third parties.[61]

Driver's Privacy Protection Act

The Driver's Privacy Protection Act of 1994 (DPPA)[62] protects the privacy of personal information assembled by state departments of motor vehicles (DMVs).

The DPPA prohibits the release or use by any state DMV (or any officer, employee, or contractor thereof) of personal information about an individual obtained by the DMV in connection with a motor vehicle record, subject to certain exceptions, such as for legitimate government needs. It sets penalties for violations and makes violators liable on a civil action to the individual to whom the released information pertains.[63]

DPPA also requires states to obtain permission from individuals before their personal motor vehicle record may be sold or released to third-party marketers.[64]

Family Educational Rights and Privacy Act

---

[56] International Council for Harmonisation, https://www.ich.org/ (last visited Mar. 25, 2023).
[57] 15 U.S.C. s. 1681.
[58] The Federal Trade Commission, Fair Credit Reporting Act, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act (last visited Mar. 25, 2023).
[59] 15 U.S.C. s. 6801.
[60] The Federal Trade Commission, Gramm-Leach-Bliley Act, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Mar. 25, 2023).
[61] International Association of Privacy Processionals, *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, https://iapp.org/media/pdf/knowledge_center/brief_requirements_GLBA.pdf (last Mar. 25, 2023).
[62] 18 U.S.C. s. 2721.
[63] 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. 25, 2023).
[64] *Id*.

The Family Educational Rights and Privacy Act (FERPA)[65] protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when they reach the age of 18 or attend a school beyond the high school level.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA.[66]

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA)[67] 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.

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.[68]

COPPA requires covered entities to:[69]

- 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 may therefore be 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.[70]

Effects of Social Media on Children

Generally, social media use by children can have both positive and negative effects on their health.[71] Some potential safety risks of social media use include:[72]

---

[65] 20 U.S.C. s. 1232(g); 34 C.F.R. s. 99.
[66] United States Department of Education, Family Educational Rights and Privacy Act (FERPA), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (last visited Mar. 25, 2023).
[67] 16 C.F.R. pt. 312.
[68] 15 U.S.C. ss. 6502(a)-(b).
[69] *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. 25, 2023).
[70] 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. 25, 2023).
[71] Mayo Clinic Staff, *Teens and social media use: What's the impact?*, Mayo Foundation for Medical Education and Research, https://www.mayoclinic.org/healthy-lifestyle/tween-and-teen-health/in-depth/teens-and-social-media-use/art-20474437 (last visited Mar. 29, 2023).
[72] Loyola Medicine, *Social Media Safety for Kids and Teens*, https://www.loyolamedicine.org/about-us/blog/social-media-safety-kids-teens, (last visited Mar. 29, 2023)

- Exposure to harmful or inappropriate content.
- Exposure to dangerous people.
- Cyberbullying.
- Oversharing personal information.
- Exposure to excessive advertisements.
- Privacy concerns, including the collection of data about minors.
- Identity theft or being hacked.
- Interference with sleep, exercise, homework, or family activities.

While children generally become more attuned to social interactions as they enter adolescence, those who are frequent, early social media users become particularly sensitive to anticipating social risks and rewards from their peers, according to a study published in JAMA Pediatrics.[73]

The researchers found that "habitual" social media users, or those who checked their social feeds 15 times a day or more, responded quicker and more intensely to perceived good or bad emotions from peers, compared to students who checked once a day or less. The areas of the brain associated with motivation and cognitive control became more active among the habitual students when expecting social rewards and punishments. The students who used little social media reacted less strongly to social cues over the same time period.[74]

Another study in the Journal of Adolescent Health found that 9- and 10-year-olds who spent hours a day playing video games or watching online algorithm-based videos had a higher risk of developing obsessive-compulsive disorders.[75]

In 2021, the Wall Street Journal reported internal research showing that Instagram conducted online surveys, diary studies, focus groups and large-scale questionnaires, which showed that 32% of teenage girls reported that Instagram made them have a worse body image. Of research participants who experienced suicidal thoughts, 13% of British teens and 6% of American teens directly linked their interest in suicide to Instagram.[76]

Recently, U.S. Surgeon General Vivek Murthy remarked that 13 years old is "too early" for children to use social media, despite most social media companies allowing 13 year olds to use their platforms. In early adolescence, kids are still "developing their identity, their sense of self," Murthy said on CNN's "Newsroom" on Jan. 29. He stated that "the skewed, and often distorted, environment of social media often does a disservice to many of those children."[77]

However, social media can allow teens to create online identities, communicate with others, and build social networks, which can provide teens with valuable support, especially helping those who experience exclusion. Social media can expose teens to current events, allow them to interact across geographic barriers, and teach them about a variety of subjects, including healthy behaviors. Also,

---

[73] Sarah D. Sparks, *Preteens" Social Media Habits Could Be Changing Their Brains*, Education Week, Jan. 6, 2023, https://www.edweek.org/leadership/preteens-social-media-habits-could-be-changing-their-brains/2023/01 (last visited Mar. 1, 2023); Maria T. Maza, BS; Kara A. Fox, MA; Seh-Joo Kwon, BS; et al, *Association of Habitual Checking Behaviors on Social Media With Longitudinal Functional Brain Development*, JAMA Pediatrics, Jan. 3, 2023, https://jamanetwork.com/journals/jamapediatrics/article-abstract/2799812 (last visited Mar. 29, 2023).

[74] Maria T. Maza, *supra* note 73.

[75] *Id*; Jason M. Nagata, M.D., M.Sc.; Jonathan Chu; Gabriel Zamora; Caitlin R. Costello, M.D.; Stuart B. Murray, D.Clin.Psych., Ph.D.; Fiona C. Baker, Ph.D.; *Screen Time and Obsessive-Compulsive Disorder Among Children 9–10 Years Old: A Prospective Cohort Study*; Journal of Adolescent Health, Dec. 12, 2022; https://www.jahonline.org/article/S1054-139X(22)00722-4/fulltext (last visited Mar. 29, 2023).

[76] Taylor Hatmaker, *Facebook knows Instagram harms teens. Now, its plan to open the app to kids looks worse than ever*, TechCrunch.com, https://techcrunch.com/2021/09/16/facebook-instagram-for-kids-mosseri-wsj-teen-girls/ (last visited Mar. 29, 2023).

[77] Lauraine Langreo, EducationWeek, *Surgeon General: Kids Under 14 Should Not Use Social Media,* Feb. 2, 2023, https://www.edweek.org/leadership/surgeon-general-kids-under-14-should-not-use-social-media/2023/02 (last visited Mar. 29, 2023).

social media that is humorous or provides a meaningful connection to peers may help teens avoid depression.[78]

In 2022, the Pew Research Center conducted a survey asking teens of their views on social media. Generally, they credit social media for helping to build stronger friendships and exposing them to a more diverse world, but they express concern that these sites lead to drama and social pressure.[79]

In addition to California's CAADCA, Utah and Arkansas have recently passed similar laws regarding children's use of social media, and several states have similar active legislation.[80]

Consumer Data Privacy – Effect of the Bill

The bill titles the act the "Florida Digital Bill of Rights."

Definitions

The bill defines the following terms:

- "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or that shares common branding with another legal entity. For purposes of this subsection, the term "control" or "controlled" means any of the following:
  - The ownership of, or power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company.
  - The control in any manner over the election of a majority of the directors or of individuals exercising similar functions.
  - The power to exercise controlling influence over the management of a company.
- "Aggregate consumer information" means information that relates to a group or category of consumers, from which the identity of an individual consumer has been removed and is not reasonably capable of being directly or indirectly associated or linked with any consumer, household, or device. The term does not include information about a group or category of consumers used to facilitate targeted advertising or the display of ads online. The term does not include personal information that has been deidentified.
- "Authenticate" or "authenticated" means to verify or the state of having been verified, respectively, through reasonable means that the consumer who is entitled to exercise consumer's rights is the same consumer exercising those consumer rights with respect to the personal data at issue.
- "Biometric data" means data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs, video or audio recordings or data generated from video or audio recordings, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.
- "Child" means an individual younger than 18 years of age.
- "Consent" when referring to a consumer, means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative act. The term does not include any of the following:
  - Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information.

[78] Mayo Clinic, *supra* note 71.
[79] Pew Research Center, *Teens' Social Media Habits and Experiences,* https://www.pewresearch.org/internet/2018/11/28/teens-social-media-habits-and-experiences/, (last visited Mar. 29, 2023).
[80] Husch Blackwell, *2023 State Children's Privacy Law Tracker, A Comprehensive Resource for Tracking U.S. State Children's Data Privacy Legislation*, https://www.huschblackwell.com/2023-state-childrens-privacy-law-tracker (last visited May 11, 2023).

- Hovering over, muting, pausing, or closing a given piece of content.
- Agreement obtained through the use of dark patterns.

- "Consumer" means an individual who is a resident of or is domiciled in this state acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context.
- "Controller" means:
  - A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:
    - Is organized or operated for the profit or financial benefit of its shareholders or owners;
    - Conducts business in this state;
    - Collects personal data about consumers, or is the entity on behalf of which such information is collected;
    - Determines the purposes and means of processing personal data about consumers alone or jointly with others;
    - Makes in excess of $1 billion in global gross annual revenues; and
    - Satisfies at least one of the following:
      - Derives 50 percent or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online;
      - Operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation. For purposes of this sub-subparagraph, a consumer smart speaker and voice command component service does not include a motor vehicle or speaker or device associated with or connected to a vehicle which is operated by a motor vehicle manufacturer or a subsidiary or affiliate thereof; or
      - Operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.
  - Any entity that controls or is controlled by a controller. As used in this paragraph, the term "control" means:
    - Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller;
    - Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
    - The power to exercise a controlling influence over the management of a company.
- "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. The term includes any practice the Federal Trade Commission refers to as a dark pattern.
- "Decision that produces a legal or similarly significant effect concerning a consumer" means a decision made by a controller which results in the provision or denial by the controller of any of the following:
  - Financial and lending services.
  - Housing, insurance, or health care services.
  - Education enrollment.
  - Employment opportunities.
  - Criminal justice.
  - Access to basic necessities, such as food and water.
- "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual.
- "Personal data" means any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that

reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

- "Political organization" means a party, a committee, an association, a fund, or any other organization, regardless of whether incorporated, organized and operated primarily for the purpose of influencing or attempting to influence any of the following:
    - The selection, nomination, election, or appointment of an individual to a federal, state, or local public office or an office in a political organization, regardless of whether the individual is selected, nominated, elected, or appointed.
    - The election of a presidential or vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed.
- "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, which directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. The term does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility.
- "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.
- "Processor" means a person who processes personal data on behalf of a controller.
- "Profiling" means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
- "Pseudonymous data" means any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.
- "Publicly available information" means information lawfully made available through government records, or information that a business has a reasonable basis for believing is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.
- "Sale of personal data" means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include any of the following:
    - The disclosure of personal data to a processor who processes the personal data on the controller's behalf.
    - The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer.
    - The disclosure of information that the consumer:
        - Intentionally made available to the general public through a mass media channel; and
        - Did not restrict to a specific audience.
    - The disclosure or transfer of personal data to a third party as an asset that is part of a merger or an acquisition.
- "Search engine" means technology and systems that use algorithms to sift through and index vast third-party websites and content on the Internet in response to search queries entered by a user. The term does not include the license of search functionality for the purpose of enabling the licensee to operate a third-party search engine service in circumstances where the licensee does not have legal or operational control of the search algorithm, the index from which results are generated, or the ranking order in which the results are provided.
- "Sensitive data" means a category of personal data which includes any of the following:

    - Personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.
    - Genetic or biometric data processed for the purpose of uniquely identifying an individual.
    - Personal data collected from a known child.
    - Precise geolocation data.
- "Targeted advertising" means displaying to a consumer an advertisement selected based on personal data obtained from that consumer's activities over time across affiliated or unaffiliated websites and online applications used to predict the consumer's preferences or interests. The term does not include an advertisement that is:
    - Based on the context of a consumer's current search query on the controller's own website or online application; or
    - Directed to a consumer search query on the controller's own website or online application in response to the consumer's request for information or feedback.
- "Voice recognition feature" means the function of a device which enables the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds.

Applicability

The bill provides that the data privacy provisions apply only to a person who:
- Conducts business in this state or produces a product or service used by residents of this state; and
- Processes or engages in the sale of personal data.

The bill does not apply to any of the following:
- A state agency or a political subdivision of the state.
- A financial institution or data subject to Title V, Gramm-Leach-Bliley Act, 15 U.S.C. ss. 6801 et seq.
- A covered entity or business associate governed by the privacy, security, and breach notification regulations issued under HIPAA and the Health Information Technology for Economic and Clinical Health Act.
- A nonprofit organization.
- A postsecondary education institution.
- The processing of personal data:
    - By a person in the course of a purely personal or household activity.
    - Solely for measuring or reporting advertising performance, reach, or frequency.

The bill provides that a controller or processor that complies with the authenticated parental consent requirements of COPPA with respect to data collected online, is considered to be in compliance with any requirement to obtain parental consent.

Exemptions

The bill exempts the following:
- Protected health information under HIPAA.
- Health records.
- Patient identifying information.
- Identifiable private information:
    - For purposes of the federal policy for the protection of human subjects;
    - Collected as part of human subjects research under the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the protection of human subjects; or
    - That is personal data used or shared in research conducted in accordance with this part or other research conducted in accordance with applicable law.

- Information and documents created for purposes of the Health Care Quality Improvement Act.
- Patient safety work product for purposes of the Patient Safety and Quality Improvement Act.
- Information derived from any of the health-care-related information listed in this section which is deidentified in accordance with the requirements for deidentification under HIPAA.
- Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section which is maintained by a covered entity or business associate as defined by HIPAA or by a program or a qualified service organization.
- Certain health Information included in a limited data set disbursed for certain health-related purposes, to the extent that the information is used, disclosed, and maintained in the manner specified by applicable health information privacy laws.
- Information used only for public health activities and purposes.
- Information collected or used only for public health activities and purposes as authorized by HIPAA.
- The collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, or by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act.
- Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act.
- Personal data regulated by the Family Educational Rights and Privacy Act.
- Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act.
- Data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.
- Data processed or maintained as the emergency contact information of an individual under this part which is used for emergency contact purposes.
- Data that is processed or maintained and that is necessary to retain to administer benefits for another individual which is used for the purposes of administering those benefits.
- Personal data collected and transmitted which is necessary for the sole purpose of sharing such personal data with a financial service provider solely to facilitate short-term, transactional payment processing for the purchase of products or services.
- Personal data collected, processed, sold, or disclosed in relation to price, route, or service as those terms are used in the Airline Deregulation Act, by entities subject to that act, to the extent the provisions of this act are preempted.
- Personal data shared between a manufacturer of a tangible product and authorized third-party distributors or vendors of the product, as long as such personal data is used solely for advertising, marketing, or servicing the product that is acquired directly through such manufacturer and such authorized third-party distributors or vendors. Such personal data may not be sold or shared unless otherwise authorized.

Consumer Rights

The bill provides that a consumer is entitled to exercise the consumer rights authorized by the bill at any time by submitting a request to a controller which specifies the consumer rights that the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise these rights on behalf of the child.

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

- To confirm whether a controller is processing the consumer's personal data and to access the personal data.

- To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.
- To delete any or all personal data provided by or obtained about the consumer.
- To obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format.
- To opt out of the processing of the personal data for purposes of:
    - Targeted advertising;
    - The sale of personal data; or
    - Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer.
- To opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data.
- To opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

The bill provides that a device that has a voice recognition feature, a facial recognition feature, a video recording feature, an audio recording feature, or any other electronic, visual, thermal, or olfactory feature that collects data may not use those features for the purpose of surveillance by the controller, processor, or affiliate of a controller or processor when such features are not in active use by the consumer, unless otherwise expressly authorized by the consumer.

Consumer Requests

The bill provides that, except as otherwise provided, a controller must comply with a request submitted by a consumer to exercise the consumer's rights.

The bill requires a controller to respond to the consumer request without undue delay, which may not be later than 45 days after the date of receipt of the request. The controller may extend the response period once by an additional 15 days when reasonably necessary, considering the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial 45-day response period, with the reason for the extension.

If a controller cannot take action regarding the consumer's request, the controller must inform the consumer without undue delay, which may not be later than 45 days after the date of receipt of the request, of the justification for the inability to take action on the request and provide instructions on how to appeal the decision. A controller is not required to comply with a consumer request submitted under if the controller cannot authenticate the request. However, the controller must make a reasonable effort to request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request. If a controller maintains a self-service mechanism to allow a consumer to correct certain personal data, the controller may deny the consumer's request and require the consumer to correct his or her own personal data through such mechanism.

The bill requires a controller to provide the consumer with notice within 60 days after the request is received that the controller has complied with the consumer's request.

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

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

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

The bill requires a controller to establish two or more methods to enable consumers to submit a request to exercise their consumer rights. The methods must be secure, reliable, and clearly and conspicuously accessible. The methods must take all of the following into account:

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

The bill prohibits a controller from requiring a consumer to create a new account to exercise the consumer's rights under this part but may require a consumer to use an existing account.

The bill requires a controller to provide a mechanism on its website for a consumer to submit a request for information required to be disclosed under the bill. A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal data may also provide an e-mail address for the submission of requests.

Appeals

The bill requires a controller to establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision.

Such appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights.

The bill requires a controller to inform the consumer in writing of any action taken or not taken in response to an appeal within 60 days after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

Waiver or limitation of consumer rights

Any provision of a contract or agreement which waives or limits in any way a consumer right under the bill is contrary to public policy and is void and unenforceable.

Controller Duties

The bill requires a controller to:

- Limit the collection of personal data to data that is adequate, relevant, and reasonably necessary in relation to the purposes for which it is processed, as disclosed to the consumer; and
- For purposes of protecting the confidentiality, integrity, and accessibility of personal data, establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue.

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

- Except as otherwise provided, process personal data for a purpose that is neither reasonably necessary nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.
- Process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

- Discriminate against a consumer for exercising any of the consumer rights, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer. A controller may offer financial incentives, including payments to consumers as compensation, for processing of personal data if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program and provided that such incentive practices are not unjust, unreasonable, coercive, or usurious in nature. The consent may be revoked by the consumer at any time.
- Process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in accordance with COPPA for a known child under the age of 13.

The bill does not require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

The bill provides that a controller that operates a search engine shall make available, in an easily accessible location on the webpage which does not require a consumer to log in or register to read, an up-to-date plain language description of the main parameters that are individually or collectively the most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. Algorithms are not required to be disclosed nor is any other information that, with reasonable certainty, would enable deception of or harm to consumers through the manipulation of search results.

Privacy Notices

The bill requires a controller to provide consumers with a reasonably accessible and clear privacy notice, updated at least annually, that includes all of the following information:

- The categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller.
- The purpose of processing personal data.
- How consumers may exercise their rights, including the process by which a consumer may appeal a controller's decision with regard to the consumer's request.
- If applicable, the categories of personal data that the controller shares with third parties.
- If applicable, the categories of third parties with whom the controller shares personal data.
- A description of the methods by which consumers can submit requests to exercise their consumer rights.

The bill requires, if a controller:

- Sells personal data to third parties or processes personal data for targeted advertising, the controller to clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process.
- Engages in the sale of personal data that is sensitive data or biometric data, the controller to provide a notice on its website alerting a consumer that it may sell such data.

The bill provides that a controller may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

Processor Duties

The bill requires a processor to adhere to the instructions of a controller and to assist the controller in meeting or complying with the controller's duties and requirements, including the following:

- Assisting the controller in responding to consumer rights requests, by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor.
- Assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor's system FIPA, taking into account the nature of processing and the information available to the processor.
- Providing necessary information to enable the controller to conduct and document data protection assessments.

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

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

The bill allows a processor to arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the bill's requirements using an appropriate and accepted control standard or framework and assessment procedure. The processor must provide a report of the assessment to the controller upon request.

This section may not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship.

A determination as to whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends on the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains in the role of a processor.

Data Protection Assessments

For processing activities generated on or after July 1, 2023, the bill requires a controller to conduct and document a data protection assessment of each of the following processing activities involving personal data:

- The processing of personal data for purposes of targeted advertising.

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

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

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

The disclosure of a data protection assessment in compliance with a request from the Attorney General does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment. A single data protection assessment may address a comparable set of processing operations which include similar activities.

A data protection assessment conducted by a controller for the purpose of compliance with any other law or regulation may constitute compliance with the data assessment requirements if the assessment has a reasonably comparable scope and effect.

Deidentified, Pseudonymous, and Aggregate Consumer Information

The bill requires a controller in possession of deidentified data to do all of the following:

- Take reasonable measures to ensure that the data cannot be associated with an individual.
- Maintain and use the data in deidentified form. A controller may not attempt to reidentify the data, except that the controller may attempt to reidentify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of this section.
- Contractually obligate any recipient of the deidentified data to comply with this part.
- Implement business processes to prevent the inadvertent release of deidentified data.

This part may not be construed to require a controller or processor to do any of the following:

- Reidentify deidentified data or pseudonymous data.
- Maintain data in an identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data.
- Comply with an authenticated consumer rights request if the controller:
    - Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

- Does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and
- Does not sell the personal data to a third party or otherwise voluntarily disclose the personal data to a third party other than a processor, except as otherwise authorized.

The bill provides that consumer rights and controller duties do not apply to pseudonymous data or aggregate consumer information in cases in which the controller is able to demonstrate that any information necessary to identify the consumer is kept separate and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

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

Sensitive Data

Any entity that is operated for profit, conducts business in this state, and collects personal data about consumers or is the entity on behalf of which such information is collected may not engage in the sale of sensitive personal data without receiving prior consent from an adult consumer, affirmative authorization from a known child who is between 13 and 18 years of age, or consent in accordance with COPPA for a known child under the age of 13.

Such entity who sells sensitive data must provide the following notice on its website: "NOTICE: This website may sell your sensitive personal data."

Exemptions for Certain Uses (s. 501.716, F.S.)

The bill does not restrict a controller's or processor's ability to do any of the following:

- Comply with federal or state laws, rules, or regulations.
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities.
- Investigate, establish, exercise, prepare for, or defend legal claims.
- Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract.
- Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis.
- Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity.
- Preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security.
- Engage in public or peer-reviewed scientific or statistical research in the public interest which adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines:
  - Whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;
  - Whether the expected benefits of the research outweigh the privacy risks; and
  - Whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.
- Assist another controller, processor, or third party in complying with the bill's requirements.

- Disclose personal data disclosed when a consumer uses or directs the controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party. An intentional interaction occurs when the consumer intends to interact with the third party, by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.
- Transfer personal data to a third party as an asset that is part of a merger, an acquisition, a bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that the information is used or shared in a manner consistent with this part. If a third party materially alters how it uses or shares the personal data of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it must provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that consumers can easily exercise choices consistent with this part.

The bill may not be construed:

- To prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.
- As imposing a requirement on controllers and processors which adversely affects the rights or freedoms of any person, including the right of free speech.
- As requiring a controller, processor, third party, or consumer to disclose a trade secret.

Collection, Use, or Retention of Data (s. 501.717, F.S.)

The bill provides that the requirements imposed on controllers and processors under the bill may not restrict a controller's or processor's ability to collect, use, or retain data to do any of the following:

- Conduct internal research to develop, improve, or repair products, services, or technology.
- Effect a product recall.
- Identify and repair technical errors that impair existing or intended functionality.
- Perform internal operations that are:
    - Reasonably aligned with the expectations of the consumer;
    - Reasonably anticipated based on the consumer's existing relationship with the controller; or
    - Otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

Th bill provides that a requirement imposed on a controller or processor does not apply if compliance with the requirement by the controller or processor, as applicable, would violate an evidentiary privilege under the laws of this state.

Disclosure of Personal Data to Third-party Controller or Processor (s. 501.718, F.S.)

A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this part does not violate this part if the third-party controller or processor that receives and processes that personal data violates this part, provided that, at the time of the data's disclosure, the disclosing controller or processor could not have reasonably known that the recipient intended to commit a violation.

A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this part may not be held liable for violations of this part committed by the controller or processor from which the third-party controller or processor receives the personal data.

Processing of Personal Data

Personal data processed by a controller pursuant to uses under s. 501.716, s. 501.717, and 501.718, F.S., may not be processed for any purpose other than those specified in those sections. Such processing may be processed to the extent that it is:

- Reasonably necessary and proportionate to the purposes of processing;
- Adequate, relevant, and limited to what is necessary in relation to the purposes of processing; and
- Done to assist another controller, processor, or third party with any of the purposes of processing.

A controller or processor that collects, uses, or retains personal data for the purposes specified in s. 501.717(1), F.S., must take into account the nature and purpose of such collection, use, or retention. Such personal data is subject to reasonable administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

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

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

A controller or processor that processes personal data pursuant to ss. 501.716, 501.717, and 501.718 bears the burden of demonstrating that the processing of the personal data qualifies for the exemption and complies with the requirements of the bill.

Enforcement and Implementation

The bill provides that if DLA has reason to believe that any person is in violation of the requirements of the bill, DLA may bring an action against such person for an unfair or deceptive act or practice under FDUTPA. A consumer may not bring an action under FDUTPA under the bill. DLA is permitted to bring an action against:

- Any person or activity regulated under laws administered by the Office of Insurance Regulation or the Department of Financial Services; and
- Banks, credit unions, and savings and loan associations regulated by the Office of Financial Regulation or federal agencies.

In addition to other remedies under FDUTPA, the department may collect a civil penalty of up to $50,000 per violation of the bill.

Civil penalties may be tripled if the violation involves:

- A consumer who is a known child. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age.
- Failure to delete or correct the consumer's personal data after receiving an authenticated consumer request or directions from a controller to delete or correct such personal data unless an exception to the requirements to delete or correct such personal data applies.
- Continuing to sell or share the consumer's personal data after the consumer chooses to opt out.

After DLA has notified a person in writing of an alleged violation, DLA may grant the person a 45-day period to cure the alleged violation. DLA may consider the number of violations, the substantial likelihood of injury to the public, or the safety of persons or property when determining whether to grant 45 days to cure. If the person cures the alleged violation to the satisfaction of DLA and provides proof, DLA may not bring an action for the alleged violation but in its discretion may issue a letter of guidance that indicates that the person will not be offered a 45-day cure period for any future violations. If the person fails to cure the violation to the satisfaction of DLA within 45 calendar days, DLA may bring an action against the person for the alleged violation. The bill clarifies that any action brought by DLA may only be brought on behalf of a Florida consumer.

DLA may adopt rules to implement the bill, including standards for authenticated consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf.

The bill requires DLA to make a report by February 1 each year publicly available on the DLA website describing any actions taken by DLA to enforce the bill. The report must include statistics and relevant information detailing:

- The number of complaints received and the categories or types of violations alleged by the complainant;
- The number and type of enforcement actions taken and the outcomes of such actions, including the amount of penalties issued and collected;
- The number of complaints resolved without the need for litigation; and
- For the report due February 1, 2024, the status of the development and implementation of rules to implement the bill.

DLA may collaborate and cooperate with other enforcement authorities of the federal government or other state governments concerning consumer data privacy issues and consumer data privacy investigations if such enforcement authorities have restrictions governing confidentiality at least as stringent as the restrictions provided in this section.

The bill provides that liability for a tort, contract claim, or consumer protection claim that is unrelated to an action brought under the bill does not arise solely from the failure of a person to comply with the bill.

The bill does not establish a private cause of action.

The bill allows DLA to employ or use the legal services of outside counsel and the investigative services of outside personnel to fulfill the obligations of the bill.

Jurisdiction

For purposes of bringing an action under the bill, any controller which collects, shares, or sells the personal data of a Florida consumer is considered to be both engaged in substantial activities within Florida, and is operating, conducting, engaging in, or carrying on a business, and doing business in Florida; and is therefore subject to the jurisdiction of Florida courts.

Preemption

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

Legal Affairs Revolving Trust Fund

The bill provides that all moneys recovered by the Attorney General for attorney fees, costs, and penalties in an action for a violation of the data privacy provisions and the Protection of Children in Online Spaces Act (PCOSA) must be deposited in the fund in the State Treasury the Legal Affairs Revolving Trust Fund, from which the Legislature may appropriate funds for the purpose of funding investigation, prosecution, and enforcement by the Attorney General.

Comparison of Consumer Data Privacy Laws[81]					
Provision	**Colorado**	**Virginia**	**California**	**European Union**	**2023 SB 262**
Opt-In or Opt-Out of Sale of PI	Opt-Out	Opt-Out	Opt-Out	Opt-In	Opt-Out
Opt-In or Opt-Out of Sensitive Info. Processing	Opt-In	Opt-In	Opt-Out	Opt-In	✓
Cure Period	✓ **60 Days (Repeals 2025)**	✓ **30 Days**	✓ **30 Days**	X	✓ **45 Days (AG Discretion)**
Right to Appeal Denials or Requests	✓	✓	X	X	✓
Express Obligations for Deidentified Data	✓	✓	X	X	✓
Requirement of Data Assessments	✓	✓	✓	✓	✓
Private Right of Action	X	X	✓ **Fine or actual damages**	✓ **Actual damages**	X
Government Enforcement Agency	Attorney General	Attorney General	Attorney General, CPPA	Information Commissioner	Attorney General
Government Enforcement Penalties	Up to $20,000 per violation	Up to $7,500 per violation	Up to $2,500 per unintentional violation, and up to $7,500 per intentional violation	Up to €20 million, or 4% of worldwide annual revenue per violation	Up to $50,000 per violation, which can be tripled in certain circumstances
Operative Date	07/01/23	01/01/23	01/01/23	05/25/18	07/01/24
Applicability Thresholds For Business/Controller	Either, per year: •Controls/Processes data of at least 100,000 consumers; or •Derives revenue from sale of data from at least 25,000 consumers	Either, per year: •Controls/Processes data of at least 100,000 consumers; or •Derives over 50% of rev. from sale of data from at least 25,000 consumers	Meets any of the following: •Gross ann. rev. over $25 million; •Processes 100,000 or more consumers; or •Derives at least 50% or more rev. from data	•Any E.U. business which processes consumer data; or •Any worldwide business that offers goods/services to or monitors behavior of E.U. individuals	•Global gross annual revenue over $1 billion; and either •Operates a certain smart speaker; •Derives 50% or more global annual revenue from data sales; or -Operates a certain app store.

Protection of Children in Online Spaces (PCOSA)

The bill provides the following definitions for PCOSA:

- "Child" means a consumer or consumers who are under 18 years of age.
- "Collect" means to buy, rent, gather, obtain, receive, save, store, or access any personal information pertaining to a child.
- "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice and includes, but is not limited to, any practice the FTC refers to as a "dark pattern."
- "Online platform" includes social media platforms and online gaming platforms.
- "Profiling" means any form of automated processing performed on personal information to evaluate, analyze or predict personal aspects related to a child's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
- "Sell" means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, a child's personal information or

[81] *See* JDSupra, *Virginia Is For Lovers…Of Data Privacy*, https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3879845/ (last visited Mar. 25, 2023).

information that relates to a group or category of children by an online platform to another online platform or an affiliate or third party for monetary or other valuable consideration.

- "Share" means to share, rent, release, disclose, disseminate, make available, transfer, or access a child's personal information for advertising or marketing. The term includes:
    - Allowing a third party to advertise or market based on a child's personal information without disclosure of the personal information to the third party.
    - Monetary transactions, nonmonetary transactions, and transactions for other valuable consideration between an online platform and a third party for advertising or marketing
- "Substantial harm or privacy risk to children" means the processing of personal information in a manner that may result in any reasonably foreseeable substantial physical injury, economic injury, or offensive intrusion into the privacy expectations of a reasonable child under the circumstances, including:
    - Mental health disorders or associated behaviors, including the promotion or exacerbation of self-harm, suicide, eating disorders, and substance use disorders;
    - Patterns of use that indicate or encourage addiction-like behaviors;
    - Physical violence, online bullying, and harassment;
    - Sexual exploitation, including enticement, sex trafficking, and sexual abuse and trafficking of online sexual abuse material;
    - Promotion and marketing of narcotic drugs, tobacco products, gambling, or alcohol; and
    - Predatory, unfair, or deceptive marketing practices, or other financial harms.

The bill prohibits online platforms that provide an online service, product, game, or feature likely to be **predominantly accessed by children** from:

- **Processing the personal information of any child** if the online platform has actual knowledge or willfully disregards that the processing may result in substantial harm or privacy risk to children.
- **Profiling a child** unless both of the following criteria are met:
    - The online platform can demonstrate it has appropriate safeguards in place.
    - Either of the following is true:
        - Profiling is necessary to provide the online service, product, or feature requested the aspects with which the child is actively and knowingly engaged.
        - The online platform can demonstrate a compelling reason that profiling does not pose a substantial harm or privacy risk to children.
- **Collecting, selling, sharing, or retaining any personal information** that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged, unless the online platform can demonstrate a compelling reason that it does not pose a substantial harm or privacy risk to children.
- **Use personal information of a child for any reason** other than a reason for which that personal information was collected, unless the online platform can demonstrate a compelling reason that use of the personal information does not pose a substantial harm or privacy risk to children.
- **Collect, sell, or share any precise geolocation data** of children unless the collection of that precise geolocation data is strictly necessary for the online platform to provide the service, product, or feature requested and then only for the limited time that the collection of precise geolocation data is necessary.
- Collect any precise geolocation data of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation data is being collected.
- **Use dark patterns** to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, game, or feature, to forego privacy protections, or to take any action that the online platform has actual knowledge or willfully disregards may result in substantial harm or privacy risk to children.
- Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. Such age estimate shall be proportionate to the risks and data practice of an online service, product, or feature.

The bill provides that if an online platform processes a child's personal information in a way covered by PCOSA, the online platform bears the burden of demonstrating that such processing is not in violation of the act.

The bill provides that a violation of PCOSA is an unfair and deceptive trade practice actionable under FDUTPA solely by DLA against an online platform. Any action brought by DLA may be brought only on behalf of a Florida child.

In addition to other FDUPA remedies, DLA may collect a civil penalty of up to $50,000 per violation. Civil penalties may be tripled for any violation involving a Florida child who the online platform has actual knowledge is under 18 years of age.

After DLA has notified an online platform in writing of an alleged violation, DLA may in its discretion grant a 45-day period to cure the alleged violation. If the violation is cured to the satisfaction of DLA and proof of such cure is provided, DLA may not bring an action for the alleged violation, but in its discretion may issue a letter of guidance that indicates that the online platform will not be offered a 45-day cure period for any future violations. If the online platform fails to cure the violation within 45 calendar days, DLA may bring an action against the online platform for the alleged violation.

The bill allows DLA to adopt rules to implement the bill.

The bill provides that liability for a tort, contract claim, or consumer protection claim that is unrelated to an action brought under PCOSA does not arise solely from the failure of an online platform to comply with PCOSA.

The bill provides that for purposes of bringing a PCOSA action, any person who meets the definition of online platform which operates an online service, product, game, or feature likely to be predominantly accessed by children and accessible by Florida children located in this state is considered to be both engaged in substantial and not isolated activities within this state and operating, conducting, engaging in, or carrying on a business, and doing business in this state, and is therefore subject to the jurisdiction of the courts of this state

Such enforcement actions are the exclusive remedy and PCOSA does not establish a private cause of action.

Florida Information Protection Act – Current Situation

In 2014, Florida passed the Florida Information Protection Act (FIPA).[82] FIPA requires commercial covered entities[83] and government entities which hold personal information to take reasonable measures to protect such information and report data breaches to affected consumers.[84]

FIPA defines "personal information" as:

- Online account information, such as security questions and answers, email addresses and passwords;
- An individual's first name or first initial and last name in combination with any one or more of the following:
    - A social security number;

[82] S. 501.171, F.S.; Fla. SB 1524 (2014) (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.)
[83] "Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. S. 501.171(1)(b), F.S.
[84] Florida Office of the Attorney General, *How to Protect Yourself: Data Security*, http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C (last visited Mar. 25, 2023).

- 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;
- Any medical history information; or
- An individual's health insurance identification numbers.[85]

Personal information does not include information:

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

If a breach of personal information occurs, notice must be given to each individual in Florida whose personal information was accessed as a result of the breach. If the breach affected 500 or more individuals in this state, the covered entity must also provide notice to the Department of Legal Affairs (DLA). If the breach affected more than 1,000 individuals at a single time, credit reporting agencies must be notified of such breach, with certain exceptions.[87]

FIPA expressly does not provide a private cause of action, but does authorize enforcement actions by DLA under Florida's Unfair and Deceptive Trade Practices Act (FDUTPA) against covered entities for any statutory violations.[88]

In addition to the remedies provided for under FDUTPA an entity that fails to provide the required notification of a data breach is liable for certain civil penalties assessed on a daily basis. The civil penalties for failure to notify apply per breach and not per individual affected by the breach.

Florida Information Protection Act – Effect of the Bill

The bill amends s. 501.171, F.S., to define "biometric information" as data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs, video or audio recordings or data generated from video or audio recordings, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

The bill includes biometric information and geolocation in FIPA's definition of "personal information" so that covered entities are required to notify the affected individual, DLA, and credit reporting agencies of a breach of such information paired with an individual's first name or first initial and last name.

The bill allows DLA to bring a FDUTPA action against a covered entity which fails to notify DLA of or an individual affected by a breach of biometric information or geolocation.

Government Moderation of Social Media Platforms – Current Situation

Many cities and government entities in Florida have official accounts on various social media platforms. Social media can be an effective platform for reaching citizens in to keep them informed about news and events in their communities.[89]

[85] *Id.*; s. 501.171(1)(g)1., F.S.
[86] S. 501.171(1)(g)2., F.S.
[87] S. 501.171(3)-(6), F.S.
[88] S. 501.171(9), (10), F.S.; OAG *supra* note 75.
[89] Jessica Marabella, CivicPlus, *7 Ways to Use Social Media with Your Municipal Website in 2019*, https://www.civicplus.com/blog/ce/using-social-media-with-municipal-website (last visited Mar. 25, 2023).

Government entities may not censor a constituent's post or comment based on views in public conversation or restrict access to their profile based solely on viewpoints based on certain Constitutional protections. However, certain speech is not protected under the First Amendment, and generally may be blocked, like threats.[90]

Government Moderation of Social Media Platforms – Effect of the Bill

The bill defines the following terms:

- "Social media platform" means a form of electronic communication through which users create online communities to share information, ideas, personal messages, and other content.
- "Governmental entity" means any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law, including, but not limited to, the Commission on Ethics, the Public Service Commission, the Office of Public Counsel, and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.

The bill provides that an officer or a salaried employee of a governmental entity may not use his or her position or any state resources to communicate with a social media platform to request that it remove content or accounts from the social media platform.

The bill prohibits a governmental entity, or an officer or a salaried employee acting on behalf of a governmental entity, from initiating or maintaining any agreements or working relationships with a social media platform for the purpose of content moderation.

However, these restrictions do not apply if the governmental entity or an officer or a salaried employee acting on behalf of a governmental entity is acting as part of any of the following:

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

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   There may be an increase in civil penalties collected by DLA.

2. Expenditures:

   There may be an increase of regulatory costs to DLA from implementing and enforcing the bill.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

[90] ACLU Florida, *Government Social Media Censorship*, https://www.aclufl.org/en/know-your-rights/government-social-media-censorship (last visited Mar 25, 2023).

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

The bill will require certain businesses with over $1 billion in gross annual sales and certain online platforms that are predominantly accessed by children that are in possession of personal data to implement mechanisms to effectuate the requirements of the bill, and such implementation will have a fiscal impact on such businesses. However, many of the businesses subject to the bill's requirements may have already implemented similar privacy practices based on protections required in other states and countries.

The bill may increase protections provided for personal information that may save consumers the expense of dealing with stolen personal information used to commit financial crimes. For instance, in 2021, about 15 million consumers were victims of identity theft or fraud.[91]

D. FISCAL COMMENTS:

None.

[91] John Buzzard, Javelin Strategy and Research, *2022 Identity Fraud Study: The Virtual Battleground*, https://javelinstrategy.com/2022-Identity-fraud-scams-report (last visited May 24, 2023).