Texas Data Privacy and Security Act:
Key Definitions and Obligations

By: Melissa Clark

Whitaker Chalk Swindle & Schwartz PLLC
City Club Lunch and Learn – November 9, 2023

Background – Federal

There is not an all-encompassing federal act that regulates privacy and data collection in the United States, though Congress has made attempts over the years.[1] While privacy laws in Europe largely came about to protect human rights, in the United States the privacy collection laws currently relate more to healthcare, minors, and finances.[2] Examples include: (a) COPPA, the Children's Online Privacy Protection Act of 1998, which imposes limits on data collection for individuals under the age of 13;[3] (b) FERPA, the Family Educational Rights and Privacy Act, which regulates who has access to student education records;[4] (c) HIPAA, the Health Insurance Portability and Accountability Act, which covers communications with doctors and hospitals;[5] (d) FCRA, the Fair Credit Reporting Act, which limits what consumer information credit bureaus can collect;[6] and (e) GLBA, the Gramm-Leach-Biley Act, which requires consumer financial products and services disclose how they share data and a consumer's rights to opt out of such sharing.[7]

Despite the lack of a single federal act, the Federal Trade Commission ("FTC"), has the authority to bring actions against businesses.[8] The FTC regularly brings actions to hold businesses to the requirements of COPPA, HIPAA, the Fair Credit Reporting Act and the FTC Act.[9] Under the FTC, truth-in-advertising and privacy principles apply to your websites and apps.[10] If your company collects any consumer information at all, your website or app must have a privacy policy and your company must honor its terms.[11]

---

[1] *See e.g.* Joseph Duball, *Pelosi opposes proposed American Data Privacy and Protection Act, seeks new preemption compromise* (Sept. 6, 2022), https://iapp.org/news/a/pelosi-rejects-proposed-american-data-privacy-and-protection-act-seeks-new-compromise/.
[2] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)* (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.
[3] *Id*.
[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] *See* Federal Trade Commission, *Protecting Consumer Privacy and Security*, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security; Federal Trade Commission, Legal Library: Cases and Proceedings, https://www.ftc.gov/legal-library/browse/cases-proceedings.
[9] Federal Trade Commission, Legal Library: Cases and Proceedings, https://www.ftc.gov/legal-library/browse/cases-proceedings; *See e.g. FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads* (May 25, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.
[10] *See* Federal Trade Commission, https://www.ftc.gov/business-guidance/privacy-security/consumer-privacy.
[11] *See* Federal Trade Commission, *Consumer Privacy*, https://www.ftc.gov/business-guidance/privacy-security/consumer-privacy.

Background – States

Over the last few years, several states have enacted privacy laws. Currently twelve states have passed data privacy laws.[12] Those states are: California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah and Virginia.[13] Massachusetts, New Jersey, North Carolina, and Pennsylvania all have bills in committee.[14] California's privacy act is the oldest state privacy act.[15] It was enacted in 2018 and was recently amended in 2020, with an effective date of January 1, 2023.[16] The state acts are consistent in that they all aim to protect data privacy, however the methods of protection and the rights afforded consumers vary state to state and most are not very far reaching beyond the applicable state's borders.

There are many ways in which the state laws are similar. Most of them adapt the European Union's General Data Protection Regulation (EU GDPR) definitions, such that the acts apply to "controllers" who meet certain requirements and who enter into contracts with "processors."[17] Most of the states have similar definitions for personal data and most also provide the same key exemptions for non-profits and for personal data which is already federally regulated.[18] Several states require Data Protection Assessments before processing high risk or sensitive data.[19] Nearly all of the states with enacted acts afford consumers the right to correct personal data which has been collected; there are only two which do not—Iowa and Utah.[20]

There are a handful of important differences between the state laws. There are two very important differences between California's act and the rest of the state acts. First, California's act allows for a private right of action and is considered the strongest privacy act in the United States.[21] Currently, the private right of action is only for data breaches, and not for the rest of the rights granted residents under the act.[22] There are two other states currently considering consumer

---

[12] *See* Anokhy Desai, *US State Privacy Legislation Tracker* (Aug 4, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/; Sawicki, Rachel, *Gov. Carney signs Delaware Personal Data Privacy Act, effective 2025* (Sept. 11, 2023 at 6:30PM), https://www.delawarepublic.org/politics-government/2023-09-11/gov-carrney-signs-delaware-personal-data-privacy-act-effective-2025.

[13] *See* Anokhy Desai, *US State Privacy Legislation Tracker* (Aug 4, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/; Sawicki, Rachel, *Gov. Carney signs Delaware Personal Data Privacy Act, effective 2025* (Sept. 11, 2023 at 6:30PM), https://www.delawarepublic.org/politics-government/2023-09-11/gov-carrney-signs-delaware-personal-data-privacy-act-effective-2025.

[14] Anokhy Desai, *US State Privacy Legislation Tracker* (Aug 4, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[15] *Id*.

[16] California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375), as amended by the California Privacy Rights Act, 2020 (herein after referred to as the "CCPA"), available at https://oag.ca.gov/privacy/ccpa.

[17] Augustinos, Theodore P. and Alexander R Cox, *U.S. State Privacy Laws in 2023: California, Colorado, Connecticut, Utah and Virginia* (December 2022), https://www.lockelord.com/newsandevents/publications/2022/12/us-state-privacy-laws-2023; see also Wolford, Ben, *What is the GDPR, the EU's new data protection law?,* https://gdpr.eu/what-is-gdpr/.

[18] *Id*.

[19] *Id*.

[20] Anokhy Desai, *US State Privacy Legislation Tracker* (Aug 4, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

[21] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)* (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

[22] CCPA.

privacy acts with private rights of action—Massachusetts and New Jersey—however most states have designated only the attorney general of their state as the party with the right to enforce the act.[23] Second, under the California act, children are consumers under 16 years of age.[24] The rest of the state laws use under 13 years of age.

Another difference between the state acts are the entities the acts apply to. In two states, Colorado and Washington, the acts do apply to non-profits.[25] In California, applicability is tied to either revenue of $25 million annually or processing levels of 100,000 residents annually or more than 50% of the entity's revenue is from selling or sharing private data.[26] In contrast, in Virginia, Colorado, and Connecticut, the applicability is only tied to processing.[27]

The Texas Data Privacy and Security Act

The Texas Data Privacy and Security Act (the "Act"), which goes into effect July 1, 2024, is designed to regulate "the collection, use, processing, and treatment of consumers' personal data by certain business entities."[28] Essentially, the Act applies to any person processing or engaging in the sale of personal data who either conducts business in Texas or produces a product or provides a service utilized by Texans, and which is not a small business.[29] However, small businesses are not completely exempt, as detailed below.[30]

Much like the other state's acts, there are, however, several exceptions to the Act. The Act does not apply to state agencies, financial institutions, entities covered by the Department of Health and Human Services, non-profits, institutions of higher education or electric utilities.[31] It also does not apply to information which is protected by HIPAA, other various health records, information relating to consumer's creditworthiness by a consumer reporting agency or furnisher, data regulated by other Federal Acts, information processed for the purposes of employing agents or independent contractors, and data necessary to administer benefits.[32]

A. Key Definitions

To determine the Act's applicability, it is crucial to understand a few key definitions regarding which data is protected and how it is processed. "'Personal data' means any information,

[23] Anokhy Desai, *US State Privacy Legislation Tracker* (Aug 4, 2023), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[24] CCPA.
[25] Augustinos, Theodore P. and Alexander R Cox, *U.S. State Privacy Laws in 2023: California, Colorado, Connecticut, Utah and Virginia* (December 2022), https://www.lockelord.com/newsandevents/publications/2022/12/us-state-privacy-laws-2023.
[26] CCPA.
[27] Augustinos, Theodore P. and Alexander R Cox, *U.S. State Privacy Laws in 2023: California, Colorado, Connecticut, Utah and Virginia* (December 2022), https://www.lockelord.com/newsandevents/publications/2022/12/us-state-privacy-laws-2023.
[28] Texas Data Privacy and Security Act, 88th Leg., R.S. (hereinafter referred to as the "TDPSA") (to be codified at Tex. Bus. & Com. Code § 541).
[29] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.002(a)).
[30] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.107).
[31] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.002(b)).
[32] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.003).

including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual."[33] Personal data does not include publicly available information.[34] "'Sensitive data is a category of personal data encompassing religious beliefs, race, ethnicity, sexuality, citizenship status, biometric data, geolocation data, and information from a child.[35]

Similar to the definition of Controller in the EU GDPR, a "controller" under the Act is the entity (an individual or organization) that determines the reason for processing personal data.[36] Processors are, essentially, the entity performing the data processing for the controller.[37] "'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."[38] An organization can be both a controller and a processor at the same time, depending on the function the organization is performing.[39]

The term "sale of personal data" "means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration…to a third party," except for the disclosure from a controller to a processor or from a controller to an affiliate.[40] This definition of sale is very broad. Sales could apply to businesses who utilize website analytics or businesses that engage in targeted advertising.

B. Consumer Rights

Under the Act, Consumers have the right to confirm with the controller whether the consumer's personal data is being processed, correct inaccuracies, request the controller delete data, obtain a copy of their digital data, and opt out of processing for targeted advertising, profiling, or the sale of personal data.[41]

C. Controller Obligations

The Act imposes a handful of requirements on controllers, including privacy policies, response obligations, Data Protection Assessments, and third-party contract obligations.[42] First, controllers are required to provide consumers with a privacy notice.[43] The notice must include: "(1) the categories of personal data processed by the controller…; (2) the purpose for processing personal data; (3) how consumers may exercise their rights…; (4) if applicable, the categories of personal data that the controller shares with third parties; (5) if applicable, the categories of third

[33] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(19)).
[34] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(19)).
[35] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(29)).
[36] *Compare* Article 4 of EU GDPR, available at https://advisera.com/gdpr/definitions/ *to* TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(8)).
[37] *See generally* TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(22)).
[38] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(22)).
[39] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.204(a)).
[40] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(28)).
[41] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.051(b)).
[42] *See* TDPSA (to be codified at Tex. Bus. & Com. Code §§ 541.052(c), 541.102(a), and 541.105(a)).
[43] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.102(a)).

parties with whom the controller shares personal data; and (6)…the methods…through which consumers may submit requests to exercise their rights."[44]

If the controller sells sensitive data, the following notice is required: "NOTICE: We may sell your sensitive personal data."[45] If the controller sells biometric data, the following notice is required: "NOTICE: We may sell your biometric personal data."[46]

Though this act is largely inapplicable to small businesses, small businesses must still obtain a consumer's consent before selling sensitive personal data.[47] Under the Act, consent "means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement…"[48] As such, a notice provision is inadequate to obtain a consumer's consent and it is insufficient to accept broad or general terms of use or to click closed a text box.[49] The best method to obtain consent is one that requires the consumer execute a written statement.[50]

Second, upon a consumer's request, a controller must either act or inform the consumer, no later than 45 days after the consumer's request is received by the controller, the reason the controller declined to take action.[51] "If the controller is unable to authenticate the request…, the controller is not required to comply with a consumer request…and may request that the consumer provide additional information."[52]

Third, controllers are required to conduct data protection assessments for various activities.[53] The activities include "(1) the processing of personal data for purposes of targeted advertising; (2) the sale of personal data; (3) the processing of personal data for profiling…; (4) the processing of sensitive data; and (5) any processing activities involving personal data that present a heightened risk of harm to consumers."[54] The assessments must identify and weigh the direct or indirect benefits of processing the data against the risks to consumers.[55] Though data protection assessments are confidential and exempt from public inspection, the attorney general may request the assessments pursuant to civil investigations under this act.[56]

Fourth, the contracts between controllers and processors must include "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 the controller and processor."[57] The contracts must also include several requirements of the processor, including ensuring the employees or contractors processing the data are subject to a duty of confidentiality, that the

[44] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.102(a)).
[45] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.102(b)).
[46] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.102(c)).
[47] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.107(a)).
[48] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(6)).
[49] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(6)).
[50] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.001(6)).
[51] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.052(c)).
[52] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.052(e)).
[53] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.105(a)).
[54] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.105(a)).
[55] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.105(b)).
[56] TDPSA (to be codified at Tex. Bus. & Com. Code §§ 541.105(c) and (d)).
[57] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.104(b)).

processor will return all of the data to the controller after the service is completed, that the processor will make available to the controller all of the data in the processor's possession, and that the processor will cooperate with controller.[58] Processors are also required to assist the controller in responding to requests from consumers and to provide the controllers with the information necessary to assist in data protection assessments.[59]

Lastly, the Act requires that the controller and processor comply with the parental consent requirements of COPPA.[60] COPPA requirements apply to any individuals under the age of 13.

D. Processor Obligations

Processors have fewer obligations than Controllers under the Act. Processors need to ensure that their employees and subcontractors are subject to confidentiality agreements.[61] Processors also need to assist Controllers with complying with the Act.[62] The specific duties are to assist the controller in responding to consumer requests, to notify controllers of a breach, and to provide controllers with enough information for the controller to do a data protection assessment.[63]

E. Enforcement

Unlike California's act, the Act does not include a private right of action.[64] If a person violates the Act, the attorney general can seek injunctive relief and impose a civil penalty of up to $7,500 per violation.[65] However, before bringing any action, the attorney general must notify the person of the violation and may not bring an action against the person if the person cures the violation within 30 days and provides the attorney general with written confirmation, including supportive documents, of the cure.[66] The attorney general has until July 1, 2024 to post a link on their website where consumers may obtain more information about the Act and how to submit complaints.[67]

Practical Guidance

(1) Assess the data collected by the company and its use and storage.
(2) Assess whether any of your consumers are in other states with a data privacy law.
(3) Review your website's privacy policy and update it for the required disclosures.
(4) Make sure any contracts with third party processors comply with the Act.
(5) Update internal policies and designate an employee to manage data and handle consumer data requests.

[58] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.104(b)).
[59] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.104(a)).
[60] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.005).
[61] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.104(b)(6)).
[62] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.104(a)).
[63] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.104(a)).
[64] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.156).
[65] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.155).
[66] TDPSA (to be codified at Tex. Bus. & Com. Code § 541.154).
[67] TDPSA § 5

Contact Information

Melissa Clark
Whitaker Chalk Swindle & Schwartz PLLC
301 Commerce Street, Suite 3500, Fort Worth, Texas 76102
Tel: (817) 878-0567
mclark@whitakerchalk.com