CLIENT ALERT:
Connecticut Adopts New State Data Privacy Law

By Gregory Paal *July 2022*

Omnibus state data privacy laws have come to New England. Connecticut became the fifth state nationally and the first state in the northeast to adopt an omnibus data privacy bill, the Connecticut Data Privacy Act ("CTDPA"), which will be effective as of July 1, 2023. The CTDPA is designed to protect and regulate the use and retention of the personal data of individuals who interact with large commercial entities. The law draws heavily from its predecessors, particularly the recently passed Virginia and Colorado data privacy laws, in establishing what is becoming the standard framework for American data privacy laws. Understanding the CTDPA can therefore provide substantial insight into American omnibus data privacy laws generally.

Other states are poised to follow in Connecticut's footsteps. The proposed Massachusetts data privacy bill, the Massachusetts Information Privacy and Security Act ("MIPSA"), is in committee, and at least 26 other states have considered similar bills in recent years. The data privacy laws of California, Utah, Colorado, Connecticut, and Virginia will be effective by the end of 2023. With a federal data privacy bill working its way through the legislative process and numerous states developing data privacy laws, companies that collect, store and use the personal data of their consumers should ensure that they understand and are ready to comply with relevant data privacy laws as they proliferate across the states.

Understanding Data Protection Laws

Though numerous state and federal statutes regulate some aspect of data privacy, no national data privacy bill provides a comprehensive framework for data protection rights and regulations in the U.S. In the absence of a federal omnibus data privacy law comparable to the EU's General Data Protection Regulation ("GDPR"), states have begun to adopt their own data privacy laws. Since the passage of the California Consumer Privacy Act ("CCPA") in 2018, four additional states have passed data protection legislation that provides a comprehensive framework for consumer privacy rights. This framework, which is itself modeled in part on the international standard set by GDPR, protects the data security of individuals living in the state by regulating the collection and use of the personal data of state residents by commercial entities.

Processing and Personal Data

State data privacy laws control the processing of personal data. **Processing** data refers to any operation performed on personal data, including its collection, use, storage, disclosure, sale and analysis. **Personal data** is generally defined as any information that can reasonably identify an individual, excluding information that is publicly available either through public records or by the individual's choice. Information posted

TWO OLIVER STREET • BOSTON, MA 02110
PHONE: 617.368.6890 • FAX: 617.368.6891
www.belcherfitzgerald.com

on an individual's social media profile, for example, is unprotected under the CTDPA.

Additional protections apply to **sensitive data**, which includes personal data pertaining to an individual's race, religion, disability, sexual orientation, precise geolocation and citizenship or immigration status. The CTDPA also considers biometric information to be sensitive data when it is processed to identify an individual. Biometric information is information pertaining to a person's biological characteristics other than information derived from an audio or visual recording. State privacy laws are split in how they address the personal information of minors. The CTDPA follows the Children's Online Privacy Protection Act ("COPPA"), which provides a baseline level of federal protection for the personal information of children under 13. The CTDPA treats such information as sensitive data. MIPSA, by contrast, would extend additional protections for the personal data of children ages 13 to 16. **The CTDPA only permits sensitive data to be processed when the individual consents to such processing** or, in the case of children under 13, when the child's parent or guardian consents in accordance with the parental notice requirements of COPPA.

The CTDPA also covers **profiling**, which refers to automated processing of personal data derived from analyzing the individual's activities rather than directly supplied by a consumer to facilitate a transaction, including data concerning the individual's economic situation, health, behavior, and location. Individuals have the right to opt out of profiling when it used for automated decisions that produce significant effects, including legal effects, for the individual.

Controllers and Processors

State data privacy laws regulate the relationships between individual state residents, Controllers, and the individual's data. A **Controller** is a covered entity that determines the purpose and means of processing personal data. A **Processor** is an entity that processes data on behalf of the Controller. Distinguishing a Controller from a Processor is a fact-based determination that considers the context of the processing.

Controllers that benefit from the collection and use of the personal information of an individual living in a state with an omnibus privacy law like the CTDPA may be subject to liability for processing such data unless the Controller complies with the privacy law. Though such laws contain numerous limitations and exceptions, they nevertheless effect a substantial change in the relationship between individuals and the covered entities that collect and use their personal information.

State data privacy laws subject Controllers to a suite of duties and consumer rights, while Processors are typically regulated more indirectly. The CTDPA applies relatively minimal direct regulations to Processors, in part because Processors that do not comply with their Controller's directions will be treated as Controllers for the purposes of the Processed data. Therefore, though Processors are only subject to a general duty to adhere to the Controller's instructions and assist Controllers in meeting their obligations under the law, a Processor that fails to follow the Controller's instructions is subject to the duties and liabilities of a Controller. Aside from the Processor's general duty, State privacy laws regulate Processors by

TWO OLIVER STREET • BOSTON, MA 02110
PHONE: 617.368.6890 • FAX: 617.368.6891
www.belcherfitzgerald.com

regulating key terms of the contract between a Controller and a Processor. The mandatory contractual terms must be incorporated into all subcontracts between a Processor and any entity with which the Processor contracts to perform any part of the processing under the prime contract between the Controller and the Processor. This flow down provision is intended to protect an individual's personal data regardless of whether the Controller has a direct contractual relationship with the ultimate Processor. The CTDPA also requires Processors notify Controllers when they engage subcontractors to process data.

The Scope of the Law

State data privacy laws vary in their scope and content, but the laws all provide a set of rights individuals may exercise over personal information that is held by a Controller. Additionally, state data privacy laws like the CTDPA require that Controllers provide notice to such individuals of their statutory rights and provide them a convenient and effective way of exercising their rights.

So far, no state has adopted a statute addressing all data processing in the state. Existing and proposed omnibus data privacy laws instead apply only to entities that either collect information from a threshold number of individuals or derive a significant part of their income from processing personal data. Additionally, non-profits and government entities are generally excluded from state omnibus privacy laws. The laws also generally exclude personal information that is regulated by other laws. Information that is already regulated by HIPAA, for example, is excluded from additional regulation under the CTDPA. Finally, employers should know that most state privacy laws, with the notable exception of California's CCPA, do not cover personal data acquired in an employment context.

In sum, state data privacy laws generally apply to entities processing a state resident's personal data, but only if the individual's personal data is not already regulated by existing laws and the entity collecting and processing the information is a large commercial entity or one that has oriented its business around processing personal information. The CTDPA, for example, applies to commercial entities conducting business in Connecticut that control or process the data of either (1) at least **100,000** Connecticut residents, **unless the personal data information is processed solely to complete a transaction**; or (2) at least **25,000** Connecticut residents, **if the Controller derives at least 25% of its gross revenue from the sale of personal data**. If an entity is covered by the CTDPA, then its affiliates are as well, regardless of their size. Using customer or profit thresholds to exclude smaller operations from more onerous compliance requirements is a common strategy in existing and proposed data privacy laws. MIPSA would also cover **data brokers**, which is a category of Controllers that collect and sell (1) the sensitive information at least 10,000 Massachusetts residents; or (2) the personal information of at least 10,000 Massachusetts residents with whom the Controller does not have a direct relationship. This MIPSA provision demonstrates another approach available to states developing data privacy laws, which is to target Controllers engaging in particular kinds of data processing and impose more stringent regulations on such entities.

TWO OLIVER STREET • BOSTON, MA 02110
PHONE: 617.368.6890 • FAX: 617.368.6891
www.belcherfitzgerald.com

Rights and Duties

State data privacy laws balance the protection of an individual's data and the commercial benefits of data collection by providing individuals with a limited set of rights relating to personal data held by Controllers and a set of duties Controllers owe to the individuals whose personal data is processed.

These rights and duties are largely derived from the **fair information principles** ("FIPs"), which provide bedrock values for Controllers who are developing a data processing strategy. The FIPs include notice to the individual of processing; choice for the individual as to what is processed, when and for how long information is stored; access to one's own data; ensuring the integrity and accuracy of the data that has been collected; and developing mechanisms that enforce the rules governing processing both internally by the Controller and externally by Processors. Controllers that design their data privacy programs around the FIPs are well positioned to avoid litigation and comply with data privacy laws as they proliferate.

In practice, the statutory rights and duties provided by the laws like the CTDPA build a framework referred to as "**notice and choice**," giving individuals notice of what information is being collected, how it is being processed, and some degree of choice over whether and how their information is processed. Notice and choice frameworks are predicated on transparency, which is at least theoretically provided by privacy notices that are made available when individuals begin using a service, and by ensuring that when individuals take affirmative steps to opt out of processing, such a request will generally be honored by the Controller. While this framework has been criticized by some commentators for being insufficiently protective of consumer privacy – for example, there is little evidence that privacy notices impact consumer behavior – it remains the dominant paradigm in proposed and enacted American data privacy laws.

***Consumer Rights*:** State data privacy laws provide consumers a limited set of rights over their personal data. These rights are intended to provide transparency as to what information is being collected and provide individuals with the right to limit the collection, storage and use of their personal data. The CTDPA provides individuals:

- the **right to know** what personal data is being processed and their privacy rights against the Controller, which must be communicated to the consumer by an explicit notification of rights;
- the **right to opt out** of processing, which must be at least as easy for individuals as the procedure for opting in to processing;
- the **right to delete** personal data held by a Controller;
- the **right to correct** personal data held by a Controller;
- the **right to obtain a copy** of the personal data held by a Controller, which must be provided to the individual in a usable, transferable format;
- the **right to appeal** a Controller's decision to decline an individual's request regarding one of their statutory rights, including the accompanying rights to a written explanation for the Controller's decision and, if the request is denied a second time, a link to the state Attorney General's Office website where the individual can submit a complaint; and

TWO OLIVER STREET • BOSTON, MA 02110
PHONE: 617.368.6890 • FAX: 617.368.6891
www.belcherfitzgerald.com

- the **right to nondiscrimination**, preventing Controllers from discriminating against consumers who exercise their rights in a manner that does not prevent the Controller from completing the transaction.[1]

***Controller Duties*:** Complimenting the consumer rights provided by state data privacy laws is the set of duties Controllers owe to the individuals whose data is being processed. The CTDPA imposes several duties on Controllers, including:

- the **duty to limit** collection and storage of data to only such data as is reasonably necessary to accomplish the purposes of the processing disclosed to the individual, also called **data minimization**[2];
- the **duty to disclose** to the customer what personal data is being processed and the purposes of the processing, which includes the duty to provide a clear, meaningful **privacy notice** that identifies: (a) categories of personal data being processed; (b) the purpose for the processing; (c) how an individual may exercise their rights; (d) categories of third parties with whom the Controller shares personal data; and (e) a means for the individual to contact the Controller online;
- the duty to provide an effective way for the individual to **opt out** of future processing; and
- the duty to establish **reasonable data security practices**.

The CTDPA further mandates that Controllers that enter contracts with Processors use mandatory contractual terms to impose a variety of obligations on Processors, including a term providing that, when an individual exercises one of their rights under the CTDPA against the Controller, the Controller can then exercise their contractual powers to compel the Processor and any of their subcontractors to also comply with the individual's request.

Controllers are obligated to produce written risk assessments to identify the foreseeable risks and benefits of data processing practices that present a heightened risk of harm to the individual. One assessment may address multiple comparable activities, which somewhat mitigates the administrative burden of such assessments. Activities that present a heightened risk of harm include processing personal data for targeted advertising, the sale of personal data, processing sensitive data, and processing data for the purposes of profiling when such profiling may result in substantial injury to the individual. The CTDPA also targets Controllers who use "dark patterns," i.e., product designs that undermine notice and choice by manipulating users into opting into unwanted processing or abandoning attempts to opt out, by deeming consumer consent obtained through dark patterns to be invalid.

Liability: One of the key distinguishing factors between state data privacy laws is the

[1] The CTDPA carves out an exception to the right to nondiscrimination to the extent that the Controller incentivizes consumer participation in data collection and processing through strategies like loyalty programs rewarding consumers who participate in surveys.

[2] Data minimization rules are limited by several categories of statutorily permissible uses of personal data, including compliance with law, use in litigation, use in public scientific research, internal uses, and for public health purposes.

TWO OLIVER STREET • BOSTON, MA 02110
PHONE: 617.368.6890 • FAX: 617.368.6891
www.belcherfitzgerald.com

liability a Controller faces for violation of the law. Enforcement of the various of the law state data privacy laws is overwhelmingly left to the state's Attorney General, with only California offering a limited private cause of action for individual consumers. **Violations of the state data privacy law may be prosecuted under the applicable state consumer protection act**. Companies that do not honor the representations made in their privacy notices may also be subject to FTC enforcement actions for unfair or deceptive trade practices. Controllers may also be subject to additional penalties in the event of a data breach in states where breaches may be treated as unfair trade practices under the applicable state consumer protection statute. However, under the CTDPA, Controllers and Processors that comply with the law are not responsible for violations committed by Processors or other third parties to whom they properly transmit personal data, unless they had *actual knowledge* the third party would break the law. Similarly, third parties who receive personal data from a Controller or Processor are not responsible for violations by the party from whom the third party received the data.

Aside from the existence of a private cause of action for consumers, the key distinguishing factor between state data privacy laws for liability purposes is whether they provide a mandatory right to cure to the Controller. States like Virginia and Utah provide a permanent right to cure for Controllers in violation of the law, which will likely diminish the incentive Controllers have to proactively comply with the law. In contrast, **the CTDPA provides an initial 60-day right to cure, but that provision sunsets on January 1, 2025**. After that point, cure periods will be available only at the discretion of the Connecticut Attorney General. While it remains to be seen whether Connecticut stridently enforces the CTDPA, the lack of a mandatory cure period amplifies the risk of non-compliance. This will also enable Connecticut to engage in effective multi-state litigation with the states that do not provide a mandatory right to cure, currently only Connecticut and California.

Looking ahead

The CTDPA is the latest in a growing list of state data privacy laws that broadly use the same structure. As more competing state-level privacy laws are enacted, it is likely that pressure will mount on the federal government to pass a national data privacy law to ease the compliance burden on multi-state Controllers and provide a baseline level of protection to individuals across the country. A bipartisan federal data privacy law has already moved out of committee and is expected to be voted on in the U.S. Senate in the near future, though commentators are skeptical that the bill will pass. In the meantime, companies that are active in states that have passed data privacy laws should consult with counsel to ensure that they will be in compliance when the law comes into effect. Other companies, particularly companies that handle large volumes of individual data, should say alert for changes to the laws controlling their business as more states adopt omnibus data privacy laws.

***

TWO OLIVER STREET • BOSTON, MA 02110
PHONE: 617.368.6890 • FAX: 617.368.6891
www.belcherfitzgerald.com