AN A.S. PRATT PUBLICATION
OCTOBER 2022
VOL. 8 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 8** **October 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Connecticut Moves to Protect Consumer Privacy: What Does Its Data Privacy Act Require?

By Jami Vibbert, Nancy L. Perkins and Jason T. Raylesberg*

The authors explain what steps businesses should take to prepare for Connecticut's new consumer privacy law.

Connecticut Governor Ned Lamont has signed into law the Act Concerning Personal Data Privacy and Online Monitoring (the "Act" or "CTDPA"), making Connecticut the fifth state to enact a broadly applicable consumer privacy law, following California, Virginia, Colorado, and Utah. Although the CTDPA bears substantial resemblance to those other states' consumer privacy laws – particularly the Colorado Privacy Act ("CPA") – businesses should take note of key distinctions among them as they prepare for compliance with the Act, which will become effective July 1, 2023.

The Act is enforceable by Connecticut's attorney general, and, like the Utah Consumer Privacy Act ("UCPA"), Virginia's Consumer Data Protection Act ("VCDPA"), and the CPA, does not empower consumers (as defined below) with a private right of action. In line with the CPA, until January 1, 2025, controllers will be afforded with a 60-day opportunity to cure a violation if the attorney general concludes a cure is possible. After January 1, 2025, the attorney general has discretion regarding whether to provide an opportunity to cure.

The Act appears to be just a first step in Connecticut's expansion of privacy regulation: the Act provides for the establishment of a task force, chaired by members of the state General Assembly and including representatives from business, academia, consumer advocacy groups, and the office of state attorney general, to study a range of privacy-related topics and to report, no later than January 1, 2023, on their findings and recommendations for possible expansion of the scope of the Act.

---

* Jami Vibbert, a partner in the New York office of Arnold & Porter Kaye Scholer LLP, helps clients navigate global data protection, privacy, and cybersecurity concerns across a number of industries, including life sciences, healthcare, financial services, media and technology. Nancy L. Perkins, counsel in the firm's office in Washington, D.C., focuses her practice on regulatory compliance and consulting on emerging policy issues, with a principal emphasis on data privacy and security and electronic transactions. Jason T. Raylesberg, an associate in the firm's New York office, advises clients on a variety of privacy, data security and consumer protection issues arising from the use of personal information. The authors may be contacted at jami.vibbert@arnoldporter.com, nancy.perkins@arnoldporter.com and jason.raylesberg@arnoldporter.com, respectively.

WHO IS SUBJECT TO THE ACT?

Like the VCDPA, CPA, UCPA, and Europe's General Data Protection Regulation ("GDPR"), the Act categorizes entities handling "personal data" as either "controllers" or "processors." Controllers are individuals or entities that determine the purpose and means of processing personal data (while it does not mean "owner," a controller is typically the entity that has rights with respect to the personal data at issue), while processors are those who process such personal data on a controller's behalf (processors are service providers or vendors). The CTDPA applies to controllers that either conduct business in Connecticut or produce products or services that are targeted to Connecticut residents and that, during the preceding calendar year, either (1) controlled or processed the personal data of at least 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, or (2) controlled or processed the personal data of at least 25,000 consumers and derived more than 25 percent of gross revenue from the sale of personal data. Thus, unlike the California and Utah models, the Act does not reach controllers solely by virtue of an annual revenue threshold.

The "sale of personal data" is defined broadly as a controller's "exchange of personal data for monetary or other valuable consideration," but does not include disclosures: (i) to the controller's processors or affiliates, (ii) pursuant to the consumer's direction, (iii) that involve only personal data already made public by the consumer, or (iv) made as part of a transaction in which the recipient of the data acquires the data as an asset along with control over all or part of the controller's assets.

"Consumers" are residents of Connecticut, but only to the extent they are acting in a personal capacity and not as employees or job applicants of a controller/processor. Specifically, an individual is not a "consumer" with respect to personal data processed in the context of that individual's employment or in the context of the individual's representation (whether as an employee, owner, director, officer, or contractor) of an organization whose "communications or transactions with the controller occur solely within that context of that individual's role with" the organization. These exclusions are similar to those under the other four states' consumer privacy laws, and underscore the legislators' intent to focus privacy protection on the personal data individuals share for personal, family, or household purposes as opposed to what they may share for employment purposes or as the representative of a company or other organization.

WHAT INFORMATION IS COVERED?

The CTDPA borrows the broad definition of "personal data" used in the UCPA, CPA, and VCDPA (and one similar to the definition in the California Consumer Privacy Act ("CCPA") and GDPR): "[A]ny information that is linked or reasonably linkable to an identified or identifiable individual" excluding de-identified data or publicly available information."

"De-identified data" is defined as "data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in" these aforementioned requirements. By requiring public commitments to process such data in a de-identified fashion without attempting re-identification, and imposing legal obligations on recipients of any such data (regardless of whether they are controllers or processors subject to the Act), the CTDPA follows the approach to de-identified data adopted in each broad consumer privacy law except for the VCDPA.

"Publicly available information" is "information that (A) is lawfully made available through federal, state, or municipal government records or widely distributed media, and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public."

WHAT EXEMPTIONS APPLY?

Consistent with the other four states' consumer privacy laws, the Act carves out from its scope certain categories of personal data and categories of entities. The majority of these carve-outs are for information or persons regulated under other privacy regimes, such as the privacy regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA") (governing "protected health information"), the Fair Credit Reporting Act ("consumer report" information), the Family Educational Rights and Privacy Act (student data), and the Children's Online Privacy Protection Act ("COPPA") (personal information collected online from children under age 13). In addition, the Act does not apply to nonprofit organizations or national securities associations registered under the Securities Exchange Act.

WHAT OBLIGATIONS DOES THE CTDPA IMPOSE?

Notice and Choice

Like each of the other state privacy regimes, the CTDPA imposes a number of obligations on both controllers and processors. Specifically, controllers must provide consumers with a "reasonably accessible and clear privacy notice" that, among other things, describes the categories of personal data processed by the controller, the purpose for processing personal data, and the categories of personal data that the controller shares with third parties, if any. To the extent a controller sells personal data to third parties or processes personal data for targeted advertising, the controller is obligated

to clearly and conspicuously disclose such processing as well as to provide a clear and conspicuous means for consumers to opt out of such processing.

Processor Contracts

Controllers must also execute written contracts with their processors that describe the nature and purpose of the planned data processing, the type of data subject to processing, and the anticipated duration of processing. Any such contract must also require that the processor, if it engages a subcontractor to assist with the data processing, (i) provide the controller with an opportunity to object, and (ii) absent an objection, bind the subcontractor to a written contract obligating the subcontractor to meet the same data protection obligations applicable to the processor with respect to the personal data.

Data Protection Assessments

Similar to the California, Colorado and Virginia state consumer privacy laws, the Act incorporates privacy by design by requiring controllers to conduct and document a data protection assessment for each of the controller's processing activities that present a "heightened risk of harm to a consumer." Examples of activities that raise heightened risks include processing personal data for purposes of targeted advertising, selling personal data, processing sensitive data (as defined below), and processing personal data for the purpose of profiling, where such profiling presents a "reasonably foreseeable risk" of unfair or deceptive treatment of or unlawful disparate impact on consumers, among other things. Such data protection assessments must identify and weigh the benefits flowing from processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer that are associated with such processing. They also must be made available to the attorney general upon request.

The CTDPA, consistent with existing broadly applicable privacy legislation, affords a special level of protection to "sensitive data." "Sensitive data" is defined as "personal data that includes (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (C) personal data collected from a known child, or (D) precise geolocation data." Controllers may not process such data without first obtaining the consent of the consumer – in the case of children's data, the consent must be obtained from a parent or guardian in accordance with rules implementing the COPPA. This opt-in requirement for processing sensitive personal data is also imposed under the VCDPA and CPA, whereas under the UCPA and the CCPA/California Privacy Rights Act ("CPRA"), a business may process sensitive personal information of a consumer unless the consumer opts out. That being said, there are several processing activities that may be undertaken without consent, even for sensitive data, assuming

they fall into one of many exclusions, which include compliance with law and internal research and development. Like the CPRA and CPA, the CTDPA explicitly excludes from the definition of "consent" any agreement obtained through the use of a "dark pattern", defined as 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 Federal Trade Commission refers to as a 'dark pattern.'" As the FTC continues to ramp up efforts to aggressively protect against dark patterns, companies should expect increased legislative and regulatory attention to these activities at both the federal and state levels.

WHAT RIGHTS CAN CONSUMERS EXERCISE UNDER THE CTDPA?

Consistent with the other states' privacy laws, the CTDPA empowers consumers with the right to access their personal data (unless such access would require the controller to reveal a trade secret), and to have the data corrected, deleted, and/or delivered in a portable format for transmission to others. Controllers must respond to consumers' requests within 45 days and without unreasonable delay. Controllers may extend the deadline for another 45 days by informing the consumer within the initial 45-day period, if it is necessary as a result of the complexity or volume of the consumer's requests. Controllers also must provide consumers with a process for appealing rejected requests.

The Act also gives consumers the right, with certain limitations, to opt out of the processing of their personal data for purposes of targeted advertising, sales, and profiling in furtherance of "solely automated decisions that produce legal or similarly significant effects concerning the consumer." By January 1, 2025, controllers subject to the CTDPA will have to incorporate a platform, technology, or other mechanism that allows a consumer to send an opt-out preference signal to the controller indicating the consumer's intent to opt out of any such processing or sale. Among other things, that platform, technology, or mechanism must not unfairly disadvantage another controller or make use of a default setting, and it must be consumer-friendly and easily usable by the average consumer.

LOOKING AHEAD

The principal challenge posed by the Act and the other similar state privacy laws for businesses to which they apply will likely be determining how to best comply with their non-uniform provisions. It is important for businesses to keep in mind that the compliance dates are fast-approaching: the CPRA (which amends the CCPA) and VCDPA are effective January 1, 2023, while the CPA and CTDPA are effective July 1, 2023, and the UCPA will come into force on December 31, 2023.