AN A.S. PRATT PUBLICATION
APRIL 2022
VOL. 8 NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 3** **April 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@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 [73] (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.

Future Proofing Privacy Compliance with Impending State Regulatory Regimes

By Alex C. Nisenbaum, Sharon R. Klein and Karen H. Shin*

This article highlights some notable differences between the applicability of the new comprehensive data privacy laws in California, Virginia and Colorado, and their requirements with respect to consumer rights, notice to consumers, vendor management and enforcement.

In 2023 comprehensive data privacy laws in California, Virginia and Colorado will go into effect, reflecting a significant and continually growing state legislative trend. With each of the laws providing for significant penalties for non-compliance, organizations are well-advised to begin preparing in 2022. The rise of comprehensive state legislation began when the California legislature hastily passed the California Consumer Privacy Act ("CCPA")[1] in 2018. In 2020, shortly after enforcement of the CCPA began, California voters approved the California Privacy Rights Act ("CPRA"), which makes sweeping amendments to the CCPA.

California was followed by Virginia and Colorado, which each passed comprehensive data privacy legislation in 2021. Similar to the privacy principles-based regulation in Europe which culminated in the General Data Protection Regulation ("GDPR"), all of these laws are designed to give consumers more control over their personal information and obligate businesses to be transparent about their privacy practices. Each law also includes unique regulatory requirements which will be challenging to operationalize across different jurisdictions. This article highlights some notable differences between the applicability of the laws and their requirements with respect to consumer rights, notice to consumers, vendor management, and enforcement.

APPLICABILITY

The CPRA becomes effective January 1, 2023. The CPRA applies to any for-profit entity doing business in California that collects or processes consumers' personal

* Alex C. Nisenbaum is a partner at Blank Rome LLP advising clients on data privacy and information security laws and regulations, including compliance with HIPAA/HITECH; Gramm-Leach-Bliley; the California Consumer Privacy Act; cross-border data transfer; and state privacy, data protection, and breach notification requirements. Sharon R. Klein is a partner at the firm advising businesses on risks related to the privacy and security of personal data, ownership, and commercialization of data artificial intelligence; privacy, security, and data protection policies and "best practices"; compliance with global, federal, and state privacy and security laws, regulations, and rules; data governance; and breach response, crisis management, and remedies for non-compliance. Karen H. Shin is an associate at the firm focusing her practice on a range of data privacy and information security matters. The authors may be reached at alex.nisenbaum@blankrome.com, sharon.klein@blankrome.com and karen.shin@blankrome.com, respectively.

[1] Cal. Civ. Code § 1798.100 et seq.

information, and: (1) has gross annual revenue in excess of $25 million in the preceding calendar year; (2) alone or in combination, annually buys, sells or shares the personal information of 100,000 or more consumers or households; or (3) derives 50 percent or more of its annual revenue from selling or sharing consumers' personal information.

The Virginia Consumer Data Protection Act ("VCDPA")[2] will take effect January 1, 2023. Entities are subject to the VCDPA if they conduct business in the Commonwealth or produce products or services that target residents of the Commonwealth, and: (a) during a calendar year, controls or processes personal data of at least 100,000 consumers, or (b) controls or processes personal data of at least 25,000 consumers and derives over 50 percent of gross revenue from the sale of personal data.

The Colorado Privacy Act ("Colo PA")[3] is effective July 1, 2023. The Colo PA applies to entities that conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to Colorado residents and: (a) controls or processes the personal data of 100,000 consumers or more during a calendar year, or (b) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.

While the applicability analysis is similar for all three states' new privacy laws, notably only California has a revenue threshold. Thus, small and medium size businesses are more likely to fall within the purview of the Virginia and Colorado laws than the CPRA.

The CPRA's regulatory framework is far reaching though in part because the definitions of "personal information" and "consumer" are incredibly broad. The CPRA defines personal information as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CPRA defines "consumer" as any California resident, but provides a limited exemption for personal information collected in employment and business-to-business contexts. These employee and business-to-business exemptions will expire on the effective date of the CPRA unless the California legislature takes action to extend them. This represents a major difference in application of the California law and Virginia and Colorado laws.

The VCDPA and Colo PA both similarly broadly define "personal data" and define "consumers" as Virginia and Colorado residents, respectively. However, the VCDPA and Colo PA completely exclude individuals acting in a commercial or employment context, job applicants and beneficiaries of individuals acting in an employment context from their definitions of consumers.

---

[2] Va. Code Ann. § 59.1-575 et seq.

[3] Colo. Rev. Stat. § 6-1-1301 et seq.

The CPRA, VCDPA and Colo PA also include the concept of sensitive personal information, which includes information revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis or sexual orientation, and processing biometric data for the purpose of uniquely identifying a natural person. Notably, the CPRA and VDCPA also include precise geolocation data in their definitions of sensitive personal information while the Colo PA does not, and the VDCPA and Colo PA include personal data collected from a known child while the CPRA does not. The CPRA further includes in its definition of sensitive personal information classic elements of state data breach notification laws – social security, driver's license, state identification card or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account – as well as the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication. The VDCPA and the Colo PA prohibit the processing of sensitive personal information without obtaining the consumer's consent, while the CPRA provides a more limited to opt out of certain uses and disclosures of sensitive personal information.

EXEMPTIONS

The CPRA, VCDPA and Colo PA generally exempt information governed by federal laws, such as information subject to the Health Insurance Portability and Accountability Act ("HIPAA"), Gramm-Leach-Bliley Act ("GLBA"), Driver's Privacy Protection Act and the Fair Credit Reporting Act ("FCRA"). However, the VCDPA and Colo PA provide for additional exemptions, including but not limited to information governed by the Family Educational Rights and Privacy Act ("FERPA"), Children's Online Privacy Protection Act ("COPPA") and Patient Safety and Quality Improvement Act. Notably, personal information subject to the GLBA or FCRA is not exempt from CPRA's private right of action in the event of a data breach.

Additionally, the CPRA, VCDPA and Colo PA exempt certain entities. The CPRA exempts non-profits, healthcare providers governed by California's Confidentiality of Medical Information Act ("CMIA"), and covered entities and business associates under HIPAA but not entities subject to the GLBA. The VCDPA exempts state bodies and agencies, financial institutions subject to the GLBA, covered entities and business associates under HIPAA, non-profits, and institutions of higher education. The Colo PA exempts financial institutions subject to the GLBA, air carriers and national securities associates registered pursuant to the Securities Exchange Act. Unlike the CPRA and VCDPA, importantly the Colo PA does not exempt non-profit entities leaving hospitals, universities, and other non-profits subject to the Colo PA.

CONSUMER RIGHTS

The CPRA, VCDPA and Colo PA provide consumers with several similar rights with respect to their personal information. Consumers in each state are afforded the rights to delete personal information, correct inaccurate personal information, know what personal information an entity is processing about the consumer, access their personal information, opt out of sale of their personal information, opt out of the use and sharing of their personal information for behavioral advertising purposes, and limit use and disclosure of their sensitive personal information.

The VCDPA and Colo PA also provide consumers the right to opt out of "profiling" that is used to make decisions that produce legal or similarly significant effects concerning the consumer. The VCDPA and Colo PA define "profiling" as any form of automated processing to evaluate, analyze, or predict personal aspects related to an individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. "Decisions that produce legal or similarly significant effects concerning a consumer" means a decision that results in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to essential goods or services. The CPRA does not include a similar right but requires the California Privacy Protection Agency to promulgate regulations governing access and opt out rights with respect to automated decision-making technology, including profiling, by July 1, 2022.

Another notable difference in the laws is regarding the right to opt-out of sale and sharing for behavioral advertising purposes. Under the Colo PA, effective July 1, 2024, consumers must be able to exercise their opt-out right through a user-selected universal opt-out mechanism that meets technical specifications to be established by the Colorado Attorney General. The Colorado Attorney General will establish the technical specifications by July 1, 2023. The California Attorney General recently announced that businesses must honor the global privacy control by treating it as an opt out. If the Colorado Attorney General adopts a different mechanism, it will mean additional work for organizations to deploy technical solutions to meet each requirement.

Under each states' law, consumer requests to exercise their rights must be verifiable and an entity may deny a consumer request if the request cannot be authenticated. Additionally, each law mandates responses to consumer rights requests within 45 days. The CPRA requires specific methods be provided to consumers for submitting requests while the VCDPA and Colo PA are not prescriptive, meaning methods used by organizations for the CCPA and CPRA can likely be leveraged across jurisdictions. Unlike the CPRA, the VCDPA and Colo PA require companies to make available an appeal process where a consumer may appeal a company's initial decision with respect to any rights' request. If the appeal is denied, the company must provide the consumer with directions about how to contact the state's Attorney General and submit a complaint.

This could prove to be a significant way for perceived issues to come to the attention of the Virginia and Colorado Attorneys General.

VENDOR MANAGEMENT

Each law requires organizations to enter into written agreements with service providers that process personal information on their behalf, but the scope of what is required in such agreements varies significantly. The VCDPA and Colo PA borrow "controller" and "processor" concepts from the GDPR and mimic the requirements of Article 28 of the GDPR by requiring nearly identical provisions to those required by the GDPR be included in contracts between controllers and processors. For instance, the agreement must set forth the type of personal data subject to the processing and the nature, the purpose and duration of the processing, only allow the processor to engage a subcontractor after the processor provides the controller an opportunity to object, and require the processor to flow down compliance obligations under the VCDPA and Colo PA to subcontractors by written agreement.

In contrast, the CPRA requires a number of unique and prescriptive terms in the written agreement between the organization and its service provider, including terms that prohibit the sale of personal information, the sharing of personal information for cross-context behavioral advertising, and combining the personal information provided by the business with other personal information from external sources, among other terms. The CPRA also requires a flow down of contractual obligations through various tiers of subcontracting. Organizations will need to review and supplement contractual terms with service providers to ensure they contain the terms mandated by each applicable law.

ENFORCEMENT AND LITIGATION

The CPRA may be enforced by the California Attorney General through a civil action, while the California Privacy Protection Agency will also have enforcement authority via administrative proceedings. Penalties of up to $2,500 for each violation and $7,500 for each intentional violation may be assessed. Unlike the CCPA, which has a 30-day cure period, the CPRA does not provide a cure period. However, like the CCPA, the CPRA provide consumers with a private right of action in the event a data breach occurs due to a business's failure to use reasonable security, and consumers may recover up to $750 per consumer per incident or actual damages, whichever is greater. The private right of action under the CCPA for data breach has fueled significant private litigation and that trend can be expected to continue under the CPRA.

Under the VCDPA, the Virginia Attorney General has exclusive enforcement authority and the Act does not provide for a private right of action. The Virginia Attorney General

must notify organizations and allow for a 30-day cure period before taking action. Civil penalties of up to $7,500 per violation plus reasonable expenses incurred in investigating and preparing the case, including attorneys' fees, may be recovered.

The Colo PA is enforced by the Colorado Attorney General and district attorneys and does not provide a private right of action. A 60-day cure period to rectify non-compliance is provided before the Colorado Attorney General or district attorney may take enforcement action. However, this cure period will only be provided until January 1, 2025. Non-compliance with the Colo PA can result in civil penalties of up to $20,000 for each violation up to a total of $500,000 for any related series of violations.

PRACTICAL TAKEAWAY

Companies subject to the California, Virginia and Colorado laws should pay close attention to the similarities and differences of these laws when developing their compliance programs as 2023 approaches. Companies should also continue to monitor the ever-evolving legal landscape of privacy, with several other states, such as Massachusetts, Minnesota, New York, North Carolina, Ohio and Pennsylvania, currently considering their own comprehensive privacy legislation.