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

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

EDITOR'S NOTE: GET READY
Victoria Prussen Spears

TOP SIX PRIVACY IMPACTS ON MOBILE HEALTH APPS FROM OVERTURNING *ROE V. WADE*
Jane E. Blaney, Peter A. Blenkinsop and Jeremiah Posedel

PREPARING FOR THE NEW AND UPDATED PRIVACY LAWS IN CALIFORNIA AND VIRGINIA
Daniel K. Alvarez, Laura E. Jehl and Stefan Ducich

THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT'S SCOPE IS SHAPED BY COURTS, WITH NO LEGISLATIVE RELIEF IN SIGHT
Kenneth K. Suh and Hannah Oswald

ARE YOU READY FOR THE BIOMETRIC TSUNAMI? THE NEW WAVE OF BIOMETRIC STATUTES
Tara L. Trifon and Brian I. Hays

CONNECTICUT MOVES TO PROTECT CONSUMER PRIVACY: WHAT DOES ITS DATA PRIVACY ACT REQUIRE?
Jami Vibbert, Nancy L. Perkins and Jason T. Raylesberg

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT: WHAT COMPANIES NEED TO KNOW NOW
Amy de La Lama, Lori Van Auken and Gabrielle A. Harwell

FEDERAL PRIVACY BILL: WILL THE UNITED STATES ENACT COMPREHENSIVE PRIVACY LEGISLATION?
Jean Paul Yugo Nagashima and Michael E. Nitardy

Pratt's Privacy & Cybersecurity Law Report

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

Editor's Note: Get Ready
Victoria Prussen Spears 257

Top Six Privacy Impacts on Mobile Health Apps from Overturning *Roe v. Wade*
Jane E. Blaney, Peter A. Blenkinsop and Jeremiah Posedel 259

Preparing for the New and Updated Privacy Laws in California and Virginia
Daniel K. Alvarez, Laura E. Jehl and Stefan Ducich 262

The Illinois Biometric Information Privacy Act's Scope Is Shaped by Courts, With No Legislative Relief in Sight
Kenneth K. Suh and Hannah Oswald 267

Are You Ready for the Biometric Tsunami? The New Wave of Biometric Statutes
Tara L. Trifon and Brian I. Hays 271

Connecticut Moves to Protect Consumer Privacy: What Does Its Data Privacy Act Require?
Jami Vibbert, Nancy L. Perkins and Jason T. Raylesberg 276

Cyber Incident Reporting for Critical Infrastructure Act: What Companies Need to Know Now
Amy de La Lama, Lori Van Auken and Gabrielle A. Harwell 281

Federal Privacy Bill: Will the United States Enact Comprehensive Privacy Legislation?
Jean Paul Yugo Nagashima and Michael E. Nitardy 287

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.

Preparing for the New and Updated Privacy Laws in California and Virginia

By Daniel K. Alvarez, Laura E. Jehl and Stefan Ducich*

In this article, the authors explain what businesses need to know to prepare for the January 1, 2023, effective date for both the California Privacy Rights Act and the Virginia Consumer Data Protection Act.

Over the last few years, privacy professionals have gained significant experience managing the uncertainties of a highly dynamic and frequently shifting regulatory and compliance landscape. Unfortunately, they will need to continue to lean on that experience, as the California Privacy Rights Act (the "CPRA") and the Virginia Consumer Data Protection Act (the "VCDPA") are scheduled to come into effect in mere months, on January 1, 2023. While a number of unknowns persist, businesses need to begin asking sometimes difficult questions – if they have not already started – about whether they are subject to these statewide comprehensive privacy laws and what steps they must take to implement appropriate internal measures and public notices that meet any new obligations.

BACKGROUND

The CPRA was adopted by California voters in November 2020 as an amendment to the California Consumer Privacy Act of 2018 (the "CCPA"). The CPRA expands consumers' rights to control their personal information, and requires businesses to implement and maintain new internal procedures and public-facing notices. On the heels of that effort, in March 2021, Virginia enacted the VCDPA, which protects consumer rights in a manner similar to the CPRA, although the scope of covered entities under VCDPA is slightly more limited.

While the CPRA and VCDPA take similarly broad approaches to data protection, specific differences between the laws persist. As to the similarities, both require covered businesses to update public notices to include certain specific practices (i.e., with respect to sensitive data), implement and maintain internal policies and procedures related to specific processing, and to execute appropriate contractual agreements. And both are

* Daniel K. Alvarez is a partner in Willkie Farr & Gallagher LLP's Communications & Media Department and co-chair of the firm's Cybersecurity & Privacy Practice Group. Laura E. Jehl is a partner in the firm's Communications & Media Department and co-chair of the firm's Cybersecurity & Privacy Practice Group. Stefan Ducich is an associate in the firm's Communications & Media Department and Cybersecurity & Privacy Practice Group. The authors may be contacted at dalvarez@willkie.com, ljehl@willkie.com and sducich@willkie.com, respectively.

likely to (continue to) produce rules, regulations and/or guidelines for businesses to comply with the laws' provisions.

However, the VCDPA and CPRA take different approaches to certain protections. For instance, each defines the scope of "sensitive data" differently (i.e., Virginia does not include government-issued ID, certain financial account information, union membership, sex-life information, or the contents of electronic communications where the business is not the intended recipient) and Virginia takes an opt-in approach to processing such data, whereas California takes an opt-out approach. State regulators have announced an intent to harmonize rules, but the lack of finalized rules thus far has complicated preparations.

There are certain questions that companies can ask to prepare for these state laws coming into force.

IS YOUR ORGANIZATION SUBJECT TO THE LAWS?

Not every organization or company that collects data from California or Virginia persons will be subject to these laws. Both the CPRA and VCDPA set threshold requirements.

Like the CCPA before it, the CPRA applies to for-profit entities (i.e., "businesses") located or doing business in California, which collect personal information from residents of the state, and which meet the minimum processing or revenue thresholds. Under the CPRA, a regulated business is one that:

- Has an annual gross revenue of over $25 million; and
- Buys, sells, or shares the personal information of at least 100,000 California consumers or households (up from 50,000 in the CCPA); or
- Derives more than fifty percent of its annual revenue from selling or sharing consumers' personal information.

The VCDPA applies to entities that conduct business in, or produce products or services targeted to residents of, Virginia, and which:

- During a calendar year, control or process the personal data of at least 100,000 Virginia consumers; or
- Control or process the personal data of at least 25,000 consumers and derive over fifty percent of their gross revenue from the sale of personal data.

Understanding whether and how these laws apply to your organization will be critical in assessing how to move forward.

WHAT DATA DOES YOUR ORGANIZATION HAVE AND WHERE DOES IT GO?

Data inventories and data-mapping exercises were among the most helpful activities for companies preparing for the effective dates of the EU General Data Protection Regulation ("GDPR") in 2018 and the CCPA in 2020. Certainly the novel aspects of these new state laws, such as the differential treatment of sensitive versus non-sensitive data under CPRA and the VCDPA, will make it important for companies that have never conducted data mapping exercises to do so, and for those that conducted such exercises a few years ago, to update them.

Identifying the collection, use and disclosure of data, in particular with respect to "sensitive personal information," automatic decision-making, and targeted advertising, will be particularly important. All of these activities will likely feed into any analysis that your organization conducts related to whether to update consumer- and public-facing notices. In Virginia, companies may also need to conduct data protection assessments – understanding when those assessments need to happen and executing them will be greatly facilitated by having previously conducted data mapping activities.

ARE YOUR VENDOR CONTRACTS COMPLIANT?

One of the key changes the CPRA makes to the CCPA is the addition of specific requirements related to vendor and other third party contracts, including specific items to be included in order to ensure that the vendor or third party is appropriately categorized. While not as specific or burdensome as GDPR's requirements for data processing contracts, these new requirements should help to ensure that a company is not unwittingly "selling" the data to its vendors.

Likewise, the VCDPA directs that any agreements with "data processors" (VCDPA imports terms like "data processor" from GDPR) must "clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties." Like GDPR, the VCDPA includes specific terms that must be included in any such agreements, which may complicate updating contracts.

IS YOUR ORGANIZATION READY TO RESPOND TO CONSUMER REQUESTS?

One of the hallmarks of the GDPR that has been imported to the U.S. in state-level comprehensive privacy laws has been the codification of consumer (or "data subject")

rights. While these concepts are not new to U.S. law – for example, some sector-specific laws already include some of these rights – these new state laws mark the first time that they have been generally available to consumers for all personal information collected by covered companies.

The CPRA expands the consumer rights established under the CCPA; to meet these obligations, businesses will need to update both their public-facing notices and their internal procedures to respond to verified consumer requests.

Among other requirements, under the CPRA businesses must:

- Provide consumers the ability to correct inaccurate personal information;
- Provide "meaningful information about the logic" used in automated decision-making, as well as access and opt-out rights for such processing;
- Notify third parties with or to whom personal information has been shared, sold, or communicated upon receipt of verifiable requests to delete personal information;
- Provide consumers with notice and the ability to opt out if the business "shares"[1] personal information; and
- Disclose how "sensitive personal information"[2] is collected, used and disclosed, and provide consumers the ability to limit the use or disclosure of this information.

The VCDPA adopts similar rights – access, opt-out, deletion, correction, and portability. Companies will need to consider how to respond to any such requests, and whether to translate any differences between the CPRA and VCDPA (and, for those companies subject to it, the General Data Protection Regulation) into different approaches to fulfilling those requests.

WHAT ABOUT EMPLOYEES?

One of the primary differences between CPRA and other recently enacted state privacy laws, including VCDPA, is that the CPRA expands the laws' requirements to the employment context (including applicants for employment, contractors, etc.) whereas VCDPA and other state laws do not. Specifically, when the CPRA takes effect, the

[1] "Sharing" is the transfer or communication of consumer personal information to a third party for cross-context behavioral advertising.

[2] "Sensitive Personal Information" includes login credentials, precise geolocation information, biometric information, genetic and health data, social security number or other government-issued identification card number, and information related to race, ethnicity, religion, or sexual orientation.

exemption under CCPA for the collection and processing of employee, applicant, and contractor personal information within the employment relationship is set to expire. This will extend consumer rights and protection obligations to employee personal information. Companies need to consider how this change will affect their operations and what additional steps they may need to take to comply.

WHAT'S NEXT?

Regulatory and enforcement authority under the CCPA was vested in the office of the California Attorney General ("CA AG"), which, since 2020, has issued certain rules pursuant to, and guidelines regarding, the law; however, this authority has now been transferred to the newly established California Privacy Protection Agency ("CPPA") (although the CA AG may still bring enforcement actions under CPRA). On July 8, 2022, the CPPA issued a Notice of Proposed Rulemaking[3] along with the proposed regulations,[4] triggering a 45-day public comment period. We expect the agency to issue regulations in several areas as we approach January 2023 and beyond. Even as companies take steps to comply with CPRA as they understand it today, they will need to monitor proceedings at the CPPA and guidance from regulators in Virginia to make sure those are appropriately incorporated into their compliance efforts.

Potential federal action further complicates the picture. For example, federal privacy legislation may also be on the horizon, with the introduction of the American Data Privacy and Protection Act ("ADPPA"). One of the mostly hotly debated issues around a comprehensive federal privacy law is whether such a law would preempt state laws such as CPRA and VCDPA; such preemption is strongly opposed by the CPPA, California's governor and much of the state's Congressional delegation. Concurrently, the Federal Trade Commission has initiated a rulemaking on "harmful commercial surveillance" and "lax data security" practices that is likely to generate significant attention. As these and similar activities make their way through their respective processes, this will be an area to watch.

Companies should also keep these questions in mind as new comprehensive privacy laws are set to come into effect in Colorado, Connecticut, and Utah beginning July 1, 2023.

---

[3] The Notice of Proposed Rulemaking is available at https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf.

[4] The Proposed Regulations are available at https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf.