

AN A.S. PRATT PUBLICATION  
NOVEMBER - DECEMBER 2022  
VOL. 8 NO. 9

PRATT'S  
**PRIVACY &  
CYBERSECURITY  
LAW**  
REPORT



**EDITOR'S NOTE: KNOCK, KNOCK**

Victoria Prussen Spears

**SEARCH WARRANTS: THE CRISIS DELIVERED  
DIRECTLY TO YOUR FRONT DOOR**

Jason P. Bologna

**PREPARE NOW TO MANAGE YOUR WORKFORCE  
THROUGH A CYBERATTACK**

Brian M. Noh

**CYBERSECURITY INSURANCE AND MANAGING  
RISK: 10 THINGS TO KNOW**

Seth Harrington, Kelly Hagedorn and Cameron Carr

**COLORADO ATTORNEY GENERAL'S OFFICE  
ISSUES DRAFT COLORADO PRIVACY ACT  
REGULATIONS**

David P. Saunders, Cathy Lee, Amy C. Pimentel and  
Elliot R. Golding

**WHAT PERSONAL INFORMATION ACCESS RIGHTS  
WILL CALIFORNIA EMPLOYEES HAVE UNDER THE  
CALIFORNIA PRIVACY RIGHTS ACT STARTING  
JANUARY 1, 2023?**

Kristen J. Mathews, Suhna Pierce and Bela Karmel

**FIRST CALIFORNIA CONSUMER PRIVACY ACT  
ENFORCEMENT ACTION SETTLEMENT AND  
SUNSETTING OF EMPLOYEE DATA EXEMPTIONS  
SIGNAL SIGNIFICANT COMPLIANCE CHALLENGES  
AHEAD**

Alex C. Nisenbaum, Sharon R. Klein, Ana Tagvoryan  
and Karen H. Shin

**THIRD CIRCUIT COURT OF APPEALS GIVES  
PENNSYLVANIA CONSUMERS NEW FOOTING FOR  
INTERNET TRACKING CLAIMS**

Thomas R. DeCesar and Jonathan R. Vaitl

**NEW YORK STATE DEPARTMENT OF FINANCIAL  
SERVICES PENALIZES CRUISE SHIP OPERATOR  
FOR FAILING TO PREVENT AND TIMELY REPORT  
CYBERATTACKS**

Celeste Koeleveld, Daniel Silver and Megan Gordon

# Pratt's Privacy & Cybersecurity Law Report

---

---

VOLUME 8

NUMBER 9

November - December 2022

---

**Editor's Note: Knock, Knock**

Victoria Prussen Spears

295

**Search Warrants: The Crisis Delivered Directly to Your Front Door**

Jason P. Bologna

297

**Prepare Now to Manage Your Workforce Through a Cyberattack**

Brian M. Noh

300

**Cybersecurity Insurance and Managing Risk: 10 Things to Know**

Seth Harrington, Kelly Hagedorn and Cameron Carr

303

**Colorado Attorney General's Office Issues Draft Colorado Privacy Act Regulations**

David P. Saunders, Cathy Lee, Amy C. Pimentel and Elliot R. Golding

307

**What Personal Information Access Rights Will California Employees Have Under the California Privacy Rights Act Starting January 1, 2023?**

Kristen J. Mathews, Suhna Pierce and Bela Karmel

312

**First California Consumer Privacy Act Enforcement Action Settlement and Sunsetting of Employee Data Exemptions Signal Significant Compliance Challenges Ahead**

Alex C. Nisenbaum, Sharon R. Klein, Ana Tagvoryan and Karen H. Shin

315

**Third Circuit Court of Appeals Gives Pennsylvania Consumers New Footing for Internet Tracking Claims**

Thomas R. DeCesar and Jonathan R. Vaitl

320

**New York State Department of Financial Services Penalizes Cruise Ship Operator for Failing to Prevent and Timely Report Cyberattacks**

Celeste Koeleveld, Daniel Silver and Megan Gordon

323

## 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)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2022 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

*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](http://www.lexisnexis.com)

MATTHEW  BENDER

(2022-Pub. 4939)

# *Editor-in-Chief, Editor & Board of Editors*

---

## **EDITOR-IN-CHIEF**

**STEVEN A. MEYEROWITZ**

*President, Meyerowitz Communications Inc.*

## **EDITOR**

**VICTORIA PRUSSEN SPEARS**

*Senior Vice President, Meyerowitz Communications Inc.*

## **BOARD OF EDITORS**

**EMILIO W. CIVIDANES**

*Partner, Venable LLP*

**CHRISTOPHER G. CWALINA**

*Partner, Holland & Knight LLP*

**RICHARD D. HARRIS**

*Partner, Day Pitney LLP*

**JAY D. KENISBERG**

*Senior Counsel, Rivkin Radler LLP*

**DAVID C. LASHWAY**

*Partner, Baker & McKenzie LLP*

**CRAIG A. NEWMAN**

*Partner, Patterson Belknap Webb & Tyler LLP*

**ALAN CHARLES RAUL**

*Partner, Sidley Austin LLP*

**RANDI SINGER**

*Partner, Weil, Gotshal & Manges LLP*

**JOHN P. TOMASZEWSKI**

*Senior Counsel, Seyfarth Shaw LLP*

**TODD G. VARE**

*Partner, Barnes & Thornburg LLP*

**THOMAS F. ZYCH**

*Partner, Thompson Hine*

---

*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. Copyright 2022 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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.

# First California Consumer Privacy Act Enforcement Action Settlement and Sunsetting of Employee Data Exemptions Signal Significant Compliance Challenges Ahead

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

*In this article, the authors discuss several recent privacy-related developments in California, and explore their implications for businesses.*

In a busy couple of weeks for California privacy, regulatory priorities came into sharp focus when California Attorney General Rob Bonta (“Attorney General”) announced the first settlement of a California Consumer Privacy Act (“CCPA”) enforcement case with Sephora, Inc. (“Sephora”) relating to its purported failure to comply with CCPA requirements regarding “sales” of personal information.

The Attorney General also provided additional summaries of other enforcement case examples where violations had been cured prior to further enforcement action.

Additionally, the California Legislature failed to pass bills extending the partial exemptions for employee personal information under the CCPA, creating additional compliance burdens for businesses with employees in California.

## **FIRST CCPA SETTLEMENT**

The Attorney General recently announced the first-ever settlement of a CCPA enforcement action. The Attorney General entered into a settlement with Sephora to resolve allegations that the company violated the CCPA. The Attorney General alleged that Sephora made certain consumer personal information it collected through its website and mobile app available to third parties, including third-party advertising networks and data analytics providers, without appropriate opt-out mechanisms in place. This allegedly included information about the products that consumers view and purchase, consumers’ geolocation data, cookies and other user identifiers, and technical information about consumers’ operating systems and browser types, which Sephora

---

\* Alex C. Nisenbaum, a partner in the Orange County office of Blank Rome LLP, advises clients on data privacy and information security laws and regulations. Sharon R. Klein, a partner in the firm’s Orange County and Los Angeles offices, is chair of the firm’s Privacy, Security & Data Protection Practice. Ana Tagvoryan, a partner in the firm’s Los Angeles office, is co-chair of the firm’s Corporate Litigation Practice Group and the firm’s Class Action Defense Team. Karen H. Shin is an associate in the firm’s Orange County office. The authors may be contacted at alex.nisenbaum@blankrome.com, sharon.klein@blankrome.com, ana.tagvoryan@blankrome.com and karen.shin@blankrome.com, respectively.

purportedly shared by installing, or allowing the installation of, cookies, pixels, and other technologies.

According to the Attorney General, Sephora's provision of information to such third parties in exchange for services from those entities was a "sale" under the CCPA in part because Sephora did not have valid "service provider" contracts in place with these third parties which, as the Attorney General noted in the settlement, is one exception to the definition of "sale" under the CCPA.

Despite engaging in these "sales," Sephora stated in its privacy policy that it did not sell personal information. Additionally, the Attorney General faulted Sephora for failing to configure its website to detect or respond to any "user-enabled privacy controls" such as the Global Privacy Control ("GPC"). Although not mentioned in the CCPA statute, the Attorney General identified user-enabled privacy controls "such as a browser plug-in or privacy setting, device setting, or other mechanism that communicate or signal the consumer's choice to opt-out" as a valid opt-out mechanism in the CCPA regulations and clarified in its CCPA FAQ in July 2021 that the Attorney General considered detecting and responding to such signals mandatory.

Sephora purportedly failed to cure the violations within the CCPA's 30-day cure period following receipt of notice of the violations from the Attorney General. In addition to CCPA violations, the Attorney General went a step further and alleged that Sephora's failure to process opt-out requests via user-enabled privacy controls and its statements that it did not sell personal information constituted unfair and deceptive practices under California's Unfair Competition Law.

As part of the settlement, Sephora will pay a penalty of \$1.2 million and maintain a two-year compliance monitoring program addressing CCPA and California Privacy Rights Act ("CPRA") compliance, including assessing and monitoring sales of personal information and processing of requests received via the GPC, and conforming its service provider agreements to CCPA's requirements.

## **UPDATED ENFORCEMENT SUMMARIES**

At the same time as the release of the Sephora settlement, the Attorney General also announced that a number of notices were sent to businesses alleging non-compliance relating to their failure to process consumer opt-out requests made via user-enabled global privacy controls, like the GPC, and updated the enforcement case examples posted on the Attorney General website.

The updated enforcement case examples illustrate a number of areas of enforcement focus, including failure to honor consumer opt-out requests, not posting a compliant notice of financial incentive, failing to provide a compliant privacy policy, and failing to appropriately honor requests to know and delete. In each of the case examples, the subject entities were able to take appropriate curative action.

However, settlements like the Sephora case may become more common for similar perceived violations in the near future as the Attorney General and the new California privacy regulator, the California Privacy Protection Agency, start to enforce the CPRA on January 1, 2023. Unlike the CCPA, the CPRA does not provide for a 30-day cure period.

## **FAILURE TO EXTEND EMPLOYEE EXEMPTION**

With the end of the California legislative session on August 31, 2022, two bills proposing to extend the CCPA exemption for information collected in the employment context failed to pass. Bill sponsors had tried two strategies: one extending the exemption indefinitely and the other until January 1, 2026. The failure of these bills results in employees, job applicants, and independent contractors being able to exercise the rights afforded to other consumers under the CCPA and CPRA as of January 1, 2023.

While these bills are presumed “dead,” they may be re-introduced with when the California Legislature reconvenes on December 5, 2022, for the 2022-2023 legislative session. By applying the privacy protections of its comprehensive privacy law to the employment context, California becomes more of an outlier among the five states that have passed comprehensive privacy legislation to date.

## **TAKEAWAYS**

While companies are busy reviewing current privacy programs to evaluate adjustments that may be required to prepare for the CPRA and other state comprehensive privacy laws, especially those effective at the start of 2023, companies should bear in mind the lessons from the enforcement activities of the Attorney General and the implications of an expansion of the CPRA to employees, job applicants, and independent contractors.

- *Ensure appropriate contracts are in place with all service providers.* The Sephora settlement confirms that “sales” under the CCPA encompass an incredibly broad array of data transfers. As the Attorney General stated, providing personal information to third parties in part of an exchange for services will come within the definition. Sephora was alleged to have transferred personal information such as geolocation data and other electronic network information to third-party web analytics and digital advertising vendors, but every transfer of personal information to a third party should be analyzed to determine if it is appropriate to categorize the third party as a “service provider” under the CCPA.

If the third party is a service provider, the business must validate that appropriate contract terms are in place as required by the CCPA. To complicate matters, the CPRA will add new contracting requirements for “service providers” and a new category of vendor, “contractors.” Businesses should be assessing their contracts now and engaging with vendors to



ensure that terms are updated appropriately in the lead up to CPRA's effective date of January 1, 2023.

- *Understand HR data flows and enhance privacy practices for employee data.* With the CCPA's partial exemption for employee, independent contractor, and applicant data now sunseting on January 1, 2023, businesses with California employees will need to extend certain privacy program processes to cover human resources data. For example, employees, independent contractors, and applicants will now be entitled to receive a full CCPA/CPRA privacy notice rather than the short form notice currently required to be provided under the partial exemption. Human resources service provider contracts will need to be reviewed and updated to include statutorily-mandated terms to avoid "sales" of human resources data. Additionally, businesses will need to prepare to receive rights requests from employees, independent contractors, and applicants relating to rights to know, delete, correct, and other rights. Businesses should review different human resources-related rights requests scenarios to test how the organization expects to respond.
- *Implement tools and processes to detect and honor global privacy controls.* While the CCPA did not include a specific requirement that GPC signals be honored as valid requests to opt-out of the sale of personal information, CCPA regulations promulgated by the Attorney General did require such capability. The Sephora settlement is the latest evidence that California regulators are likely to continue to take this requirement seriously. GPC signals allow consumers to tell every website they visit what their cookie preferences are. Businesses should assess the technical capabilities of their online points of presence to ensure they are able to honor requests sent by GPC signals. Businesses should also stay up to date with new regulations being developed by the California Privacy Protection Agency, which could provide additional technical specifications and requirements that businesses will need to implement.
- *Review privacy notices for comprehensiveness and readability.* The latest case enforcement summaries published by the Attorney General still frequently cite non-compliant privacy policies as a reason for why a business received a notice of non-compliance. Privacy policies are low hanging fruit for the Attorney General to review and assess compliance. Businesses should ensure that their public facing privacy disclosures are accurate, contain all mandated disclosures, and are understandable and not confusing. Although precise requirements for privacy notices may further evolve as the California Privacy Protection Agency continues to develop CPRA regulations, businesses should also be evaluating their current CCPA notices to determine what uplift needs to be done to make them CPRA compliant.

- *Review financial incentive programs.* Financial incentives are another area where the Attorney General has focused significant regulatory attention, including announcing an “enforcement sweep” where a number of businesses operating loyalty programs were alleged to be out of compliance with notice and opt-out requirements. The absence of a proper notice of financial incentive or the failure to provide that notice to consumers before they join the program or to obtain opt-in consent are all shortcomings that are easy to spot. Companies that operate loyalty programs or offer other financial incentives should review their notices and consumer workflows, such as how a consumer opts-in or opts-out of the program, against the Attorney General’s enforcement case examples to avoid similar issues.