

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

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



LexisNexis

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

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.

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

*By Kristen J. Mathews, Subna Pierce and Bela Karmel**

In this article, the authors discuss the scope of an employee's right to receive the personal information that the employer has about the employee.

Companies are preparing to respond to employee rights requests under the California Privacy Rights Act ("CPRA") when the law's employee exemption expires in January 2023. This article discusses the scope of an employee's right to receive the personal information that the employer has about the employee.

BACKGROUND

As of January 1, 2023, employees (including former employees, job applicants, independent contractors, business owners, directors, and officers, and any of their emergency contacts and beneficiaries) who are California residents will have the right to know about, and access, the personal information that their employer has about them.

Under these rights, an employee may request that their employer share with them:

- The categories of personal information ("PI") the employer has collected about the employee;
- The categories of sources from which the employer collected the PI;
- The employer's business or commercial purpose for collecting or selling the PI;
- The categories of third parties to whom the employer has disclosed the PI; and
- Copies of the actual PI itself that the employer has collected about that employee. This includes PI that the employer has collected *about* the employee and not only PI it has collected *from* the employee.

* Kristen J. Mathews is a partner in Morrison Foerster's Global Privacy + Data Security Group, based in the firm's office in New York. Subna Pierce, of counsel in the firm's New York office, advises clients on complying with U.S. and foreign privacy and data protection laws. Bela Karmel is an associate in the firm's Privacy + Data Security practice. The authors may be contacted at kmathews@mof.com, spierce@mof.com and bkarmel@mof.com, respectively.

The CPRA's requirements apply to PI collected on or after January 1, 2022, which limits the PI that is subject to an employee's rights.

An employee's personnel file likely contains a lot of PI about the employee that would be subject to the employee's access right. Employee PI is also likely to be stored in several other repositories that an employer maintains. Yet, these records may also contain information that is not PI about the employee or that falls within an exception to the employer's CPRA obligations. The CPRA gives employees a right to receive "specific pieces" of PI, not necessarily copies of whole documents that also contain other information about the company or about other people.

While personal information is broadly defined as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly," with the employee, it does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. This might exempt information about the employee that is publicly available on the Internet. The CPRA also does not apply to consumer reports under the Fair Credit Reporting Act or medical information covered by certain other federal and state privacy laws. Also, the PI that must be provided to the employee does not include data generated to help ensure security and integrity, so an employer may not have to provide information about an employee related to certain kinds of internal investigations.

Likewise, the CPRA does not require disclosure of PI that falls within an exception, such as if the disclosure would hinder the company's ability to comply with a federal, state, or local law, or to exercise or defend a legal claim, or if the disclosure would waive a privilege or adversely affect the rights and freedoms of other individuals. The CPRA also does not apply to PI that is adequately de-identified or aggregated, and it provides an exception for unduly burdensome requests.

However, the employer should also be mindful that the California Labor Code provides employees with the right to "inspect and receive a copy of the personnel records that the employer maintains relating to the employee's performance or to any grievance concerning the employee." An employer that receives an access request from an employee who is a California resident should identify whether the employee is making the request under the CPRA, or a request to inspect and receive personnel records under the Labor Code, or both, because this will determine what information must be provided, and the timeline for providing it.

QUESTIONS TO CONSIDER

In most cases, employers will need to look beyond the personnel file to respond to an employee's CPRA request because companies generally collect PI about employees in additional repositories. This does not mean that an employer must search for and provide every email, message, or document that mentions the employee or on which

the employee was a sender or recipient. Important questions that the company should consider include:

- What are data sources in which the company has collected PI about the employee (e.g., payroll records), as opposed to repositories containing PI that the company has not collected (e.g., an extracurricular bowling team that is not sponsored by the company that co-workers coordinate using the company's email and shared drives). This may include email servers or messaging channels that are used by the employee who made the request.
- Does the data at issue constitute PI about the employee? For example, in a list of expense reimbursements paid to multiple employees, only the information related to the requestor is PI about that employee, and any other information should be withheld. Similarly, an email that the employee sent or received that includes content that is not about the employee might be redacted down to only the employee's name and email address.
- Do any exceptions apply? For example, disclosing a record containing another employee's opinions about the requestor could adversely affect the privacy interests of the other employee. This may trigger the CPRA's exception for disclosures that adversely affect the rights and freedoms of other individuals.

CONCLUSION

It is important to note that many CPRA access requests received from employees, former employees, and employee candidates may in fact be veiled pre-litigation discovery attempts. That said, employers may not retaliate against employees for making a CPRA request. So, these requests should be handled with great care, with the involvement of both the human resources and legal departments, taking into account how the requestor and their own legal counsel may be planning to use the information they obtain through a CPRA request.