

AN A.S. PRATT PUBLICATION

JUNE 2024

VOL. 10 NO. 5

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



LexisNexis

**EDITOR'S NOTE: PRIVACY PROTECTION RULES  
CONTINUE TO GROW**

Victoria Prussen Spears

**BIDEN EXECUTIVE ORDER TO PROTECT AMERICANS'  
SENSITIVE PERSONAL DATA AND RELATED  
RULEMAKING COULD IMPOSE SIGNIFICANT  
RESTRICTIONS ON CERTAIN TRANSFERS  
OF SENSITIVE PERSONAL INFORMATION**

Jason C. Chipman, Benjamin A. Powell,  
David J. Ross, Arianna Evers and  
Ariel Dobkin

**REPORTING COMPANIES UNDER THE CORPORATE  
TRANSPARENCY ACT BEWARE: USING SERVICE  
PROVIDERS TO COMPLY CREATES NEW DATA  
PRIVACY RISK**

Mary J. Hildebrand, Robert A. Johnston Jr.  
and Judith G. Rubin

**LESS IS MORE WHEN IT COMES TO  
EMPLOYEE MONITORING**

Kathleen Grossman

**STATE HEALTH DATA PRIVACY LAWS BRING  
NOVEL COMPLIANCE CHALLENGES**

Wendell J. Bartnick, Angela Matney,  
Nancy Bonifant Halstead and  
Vicki J. Tankle

**CALIFORNIA ATTORNEY GENERAL RAMPS  
UP CALIFORNIA CONSUMER PRIVACY ACT  
ENFORCEMENT WITH DOORDASH SETTLEMENT,  
REINFORCES CALIFORNIA ONLINE PRIVACY  
PROTECTION ACT PRINCIPLES**

Madeleine Findley, Daniel R. Echeverri and  
Ginsey V. Kramarczyk

**UK'S DATA PROTECTION REGULATOR CONTINUES  
TO CLAMP DOWN ON THE USE OF BIOMETRIC  
RECOGNITION TECHNOLOGY**

Rob Dalling and Tracey Lattimer

# Pratt's Privacy & Cybersecurity Law Report

---

---

VOLUME 10

NUMBER 5

June 2024

---

<b>Editor's Note: Privacy Protection Rules Continue to Grow</b> Victoria Prussen Spears	135
<b>Biden Executive Order to Protect Americans' Sensitive Personal Data and Related Rulemaking Could Impose Significant Restrictions on Certain Transfers of Sensitive Personal Information</b> Jason C. Chipman, Benjamin A. Powell, David J. Ross, Arianna Evers and Ariel Dobkin	137
<b>Reporting Companies Under the Corporate Transparency Act Beware: Using Service Providers to Comply Creates New Data Privacy Risk</b> Mary J. Hildebrand, Robert A. Johnston Jr. and Judith G. Rubin	145
<b>Less Is More When It Comes to Employee Monitoring</b> Kathleen Grossman	148
<b>State Health Data Privacy Laws Bring Novel Compliance Challenges</b> Wendell J. Bartnick, Angela Matney, Nancy Bonifant Halstead and Vicki J. Tankle	151
<b>California Attorney General Ramps Up California Consumer Privacy Act Enforcement with DoorDash Settlement, Reinforces California Online Privacy Protection Act Principles</b> Madeleine Findley, Daniel R. Echeverri and Ginsey V. Kramarczyk	158
<b>UK's Data Protection Regulator Continues to Clamp Down on the Use of Biometric Recognition Technology</b> Rob Dalling and Tracey Lattimer	161

## 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

LexisNexis® Support Center ..... <https://supportcenter.lexisnexis.com/app/home>

For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940

Outside the United States and Canada, please call ..... (518) 487-3385

---

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (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 © 2024 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

(2024-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, Sidley Austin 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 2024 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.

# Reporting Companies Under the Corporate Transparency Act Beware: Using Service Providers to Comply Creates New Data Privacy Risk

*By Mary J. Hildebrand, Robert A. Johnston Jr. and Judith G. Rubin\**

*In this article, the authors explain that reporting companies are responsible for compliance with state, federal, or foreign data privacy and cybersecurity laws – and for ensuring that their service providers, vendors and consultants comply as well.*

The Corporate Transparency Act (CTA), which became effective on January 1, requires that U.S. and foreign companies authorized to do business in the U.S. (each, a Reporting Company) report specific personal information regarding their beneficial owners<sup>1</sup> (beneficial ownership information, or BOI) to the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) via the Beneficial Ownership Secured System (BOSS) unless an exemption applies. FinCEN has issued a series of rules<sup>2</sup> that specify Reporting Company obligations under the CTA, govern access to BOI, and revise customer due diligence rules (the latter is slated for issuance in 2024) (collectively, the FinCEN Rules).

## **BOI, IDENTIFIERS AND DATA PROTECTION LAWS**

- *Beneficial Ownership Information:* BOI includes not only personal information such as legal name, date of birth, and complete current address of a potentially large group of individuals for each Reporting Company but also sensitive personal information that requires enhanced privacy and security measures under state, federal, or foreign data privacy and cybersecurity laws (Data Protection Laws).

Specifically, the unique identification numbers from drivers' licenses, passports, or similar government-issued photo identification documents, as well as photos (images) of the documents, are highly likely to be viewed as sensitive personal information (Sensitive PII) under current Data Protection Laws in California, Virginia, Colorado, Connecticut, and Utah, and the Texas Data Privacy and Security Act (effective July 1).

---

\* The authors, attorneys with Lowenstein Sandler LLP, may be contacted at mhildebrand@lowenstein.com, rjohnston@lowenstein.com and jrubin@lowenstein.com, respectively.

<sup>1</sup> "Beneficial owners" means persons who incorporated or formed a company, who own 25 percent or more of a company, and who exert substantial control over a company.

<sup>2</sup> The Final Beneficial Ownership Information Reporting Rule, which became effective on January 1; the Final Rule on Access to Beneficial Ownership Information, which becomes effective on February 1; and a third major rule slated to be issued by FinCEN in 2024 to revise its Customer Due Diligence

Depending on a Reporting Company's business, industry, and geographic locations, BOI (including sensitive elements) may also be regulated by sector-specific federal laws (applicable, for example, to health care or financial services), regional regulations (such as the General Data Protection Regulation in the European Union), and/or other Data Protection Laws. To comply with the CTA, Reporting Companies will need to collect, process, and report BOI shortly after the company's formation<sup>3</sup> and thereafter whenever any information on a BOSS filing changes (e.g., a photo identification document expires or a home address changes).

- *FinCEN Identifiers*: Pursuant to the CTA, upon request by a beneficial owner, a company applicant (i.e., the individual who directly files the document creating the domestic Reporting Company), or a Reporting Company, FinCEN may assign a numeric identifier (FinCEN Identifier) to each natural person or entity. Company applicants and beneficial owners must provide FinCEN with the same BOI to be eligible for a FinCEN Identifier. FinCEN cannot issue more than one FinCEN Identifier to the same individual or entity (including any successor entities).

Reporting Companies may report FinCEN Identifiers instead of BOI for each beneficial owner, and company applicants may also use their own FinCEN Identifiers to avoid repeatedly providing BOI. On November 7, 2023, FinCEN issued a final rule clarifying the criteria that must be met for a Reporting Company to use a FinCEN Identifier for an intermediate entity in lieu of BOI, and additional regulations are anticipated this year.

- *Data Protection Laws*: BOI and FinCEN Identifiers are highly likely to constitute PII when collected or processed by Reporting Companies and the service providers, vendors, and consultants (Service Providers) engaged by Reporting Companies to assist with CTA compliance (CTA Services). The CTA and the FinCEN Rules create an opportunity for existing Service Providers to expand their offerings and incentivize early-stage companies and startups to pivot and enter the new market.

Service Providers that market or provide CTA Services frequently lack the robust privacy and cybersecurity infrastructure and technology platform necessary to protect and secure BOI (including Sensitive PII) as required by Data Protection Laws, leaving the Reporting Companies exposed to enhanced regulatory, legal, and commercial risks.

---

<sup>3</sup> In 2024, any company incorporated, formed, or authorized to do business in any U.S. state, territory, or tribal land by filing a document with a U.S. state secretary of state or similar authority will have 90 days to make its initial BOSS filing unless an exemption applies. For 2025 and beyond, this timeline is reduced to 30 days.

## **WHAT SHOULD REPORTING COMPANIES DO NOW?**

Reporting Companies are responsible for compliance with Data Protection Laws and for ensuring that Service Providers comply as well. It is essential that Reporting Companies:

- (1) Establish internal and external processes to identify BOI and FinCEN Identifiers as PII, regardless of the source;
- (2) Evaluate the PII and determine applicable Data Protection Laws; and
- (3) Integrate the PII into legally compliant data protection programs.

Reporting Companies should revisit their current selection and vetting process for Service Providers to include the capability to identify, evaluate, and integrate BOI and FinCEN Identifiers as PII. This includes, as applicable, providing enhanced data privacy and security measures to protect Sensitive PII. Service Providers should demonstrate their CTA resources, including relevant technology, processes, and procedures. Extra caution is advisable when Reporting Companies are urged to become “early adopters” or Service Providers emphasize the competitive nature of pricing options.

In addition to the foregoing, Reporting Companies should ensure that CTA Services are not provided (and Service Providers are not compensated) unless an agreement is in place that contractually requires Service Providers to:

- (1) Comply with Data Protection Laws applicable to the PII (specifically including BOI and FinCEN Identifiers);
- (2) Allow annual audits by the Reporting Company or its designee; and
- (3) Purchase cyber insurance that provides coverage for any security incident or data breach that affects BOI and/or FinCEN Identifiers.