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

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 9** **November - December 2022**

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.

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

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

The authors provide an overview of draft regulations recently released in Colorado to the state's privacy law.

The Colorado Attorney General's Office (the "AG's Office") has released draft regulations[1] to the Colorado Privacy Act (the "CPA"). Before these proposed regulations take effect, however, there will be a lengthy public comment period, running from October 10, 2022, through February 1, 2023.

On February 1, 2023, the AG's Office will hold a public hearing on the proposed regulations and then take the public comments under advisement. In short, we are still several months away from having finalized regulations under the CPA, which goes into effect on July 1, 2023.

The good news for businesses is that the draft regulations (1) are mostly consistent with the proposed California Consumer Privacy Act (the "CCPA") regulations, and (2) do not contain too many new obligations beyond the plain language of the CPA itself. This will hopefully ease the compliance burden for companies that are plotting out a multistate approach.

KEY DIFFERENCES FROM THE CCPA DRAFT REGULATIONS

Many of the differences between the CCPA regulations and the proposed CPA regulations are technical in nature. However, what most businesses are likely to focus on is what are the new or different things that the CPA regulations would require above and beyond what companies are already preparing for in their CCPA privacy notices. Discussed in more detail below, some of the key differences include:

- The CPA regulations require the disclosure of the new consumer right to appeal a data subject request decision of a company, a right not found in the CCPA.

---

* David P. Saunders, a partner in the Chicago office of McDermott Will & Emery, focuses his practice on privacy and cybersecurity matters. Cathy Lee, an associate in the firm's office in Washington, D.C., focuses her practice on privacy and cybersecurity matters. Amy C. Pimentel, a partner in the firm's Boston office, advises clients on global data protection, privacy and cybersecurity. Elliot R. Golding, a partner in the firm's Washington, D.C., office, provides privacy and cybersecurity advice to global companies spanning virtually every sector of the economy. The authors may be contacted at dsaunders@mwe.com, cjlee@mwe.com, apimentel@mwe.com and egolding@mwe.com, respectively.

[1] https://coag.gov/app/uploads/2022/10/CPA_SOS-notice-and-statement.pdf.

- There is significantly more detail regarding how companies will be expected to acknowledge and honor opt-out signal technology (as of 2024) as compared to the proposed CCPA regulations.

- Colorado also appears to have taken a more practical approach to loyalty programs than the CCPA. For example, there is an express recognition in the CPA regulations that if a consumer's privacy preferences make the delivery of a loyalty program benefit impossible, then companies are under no obligation to provide the benefit.

- The CPA regulations dedicate significant space and detail to the requirements for obtaining consent from a Colorado resident.

NOTABLE REQUIREMENTS IN THE CPA PROPOSED REGULATIONS

- *Instructions on Appeals Process*: Rule 6.03 would require companies to provide in their privacy notice instructions to consumers on how they may appeal a company's decision in response to a data rights request. The existence of the consumer appeal right is one of the key differences between California and the laws of Colorado, Connecticut and Virginia.

- *Authenticating Data Rights Requests*: Rule 4.08 would require companies to establish "reasonable methods" to authenticate a consumer submitting a data rights request. To determine if a method is reasonable, companies must consider the right exercised, the type, sensitivity, value and volume of personal data involved, and the level of harm that improper access or use could cause the consumer. Practically speaking, these proposed regulations allow businesses to make the CCPA's authentication requirements the floor rather than inventing a new, or worse, conflicting, process whole cloth.

- *System for Recognizing Universal Opt-Out Mechanisms*: The proposed CPA regulations provide significantly more guidance and direction to companies about honoring universal opt-out mechanisms than the draft CCPA regulations. The CPA regulations provide, for example, that the Colorado Department of Law will maintain a public list of mechanisms that have been recognized by the AG's Office as meeting the required standards for opt-out signal technology. The proposed CPA regulations also provide far greater detail than the CCPA regulations with respect to the deployment and effect of the signals. While there is room to improve still on these proposed rules, they are more detailed and pose less compliance burden than the proposed CCPA regulations.

- *Identification of Rights*: The proposed regulations largely mirror the CCPA regulations in terms of the requirements for the delivery and content of privacy notices. However, there are some specifics in the CPA-proposed regulations that will require companies' attention. For example, a privacy

policy must "clearly indicate[]" which data subject rights are available to Colorado residents. The proposed regulations also require that a company's privacy policy use the word "privacy" in the static link available on web pages. This will require a move away from the "Legal Notices" or "Terms" links that some companies use.

- *Biometrics Definitions*: Rule 2.02 would introduce new defined terms and definitions, including "Biometric Data" and "Biometric Identifiers." What is noteworthy about the definition of "Biometric Identifiers" is that it applies not just to commonly conceived concepts of biometrics but also to "behavioral characteristics." It is unclear what "behavioral characteristics" ultimately would comprise "Biometric Data" (*i.e.*, a biometric identifier used for identification purposes), but it introduces a new concept of biometrics that is less than clear.

- *Introduction of Duty Regarding Sensitive Data*: The CPA-proposed regulations would codify something that many privacy professionals had been anticipating: Sensitive data *inferences* would be treated the same way as the sensitive data itself. The classic example is that if someone tells a company that they keep a certain religious diet, the company can infer from that information a sensitive data category (e.g., religious beliefs). Rule 6.10 would provide duties regarding a company's processing of this type of inference data. In addition to obtaining consent to process these inferences, there are limits on the period of time in which they can be stored by a company.

- *Disclosures for a Request for Consent*: The proposed regulations, beginning in Rule 7.03, set forth a robust set of rules around both the method and content for obtaining consumer consent under the CPA. Some of these requirements are proscriptive, such as the requirements that consents must be combined with other consents and must contain certain disclosures. Any company that has to obtain consent under the CPA should pay close attention to these proposed regulations.

- *Refreshing Consent*: Rule 7.08 would introduce a new requirement of "refreshing consent." Under the proposed regulation, a company must refresh consent "at regular intervals." The draft regulations do not provide much clarity on how often consent should be "refreshed," simply stating that it should be based on the context and scope of the original consent, sensitivity of the personal data collected and the consumer's reasonable expectations. Rule 7.03 does require that consent must be "refreshed" annually for sensitive data.

- *Data Protection Assessments*: Rule 8.04 describes what would become of the content requirements for data protection assessments. The draft rule provides a lengthy list of 18 elements to be addressed in each assessment, including, for example, the specific purpose of the processing, procedural safeguards and the dates the assessment was reviewed and approved. In addition, the new regulations would require that these assessments be revisited and updated on at least an annual basis.

- *Profiling*: The draft regulations give particular focus to profiling. The rules distinguish between profiling based on: (i) solely automated processing; (ii) human reviewed automated processing; and (iii) human involved automated processing. Controllers that engage in profiling must provide additional disclosures in their privacy notice about this type of activity including, but not limited to:

    - What decision is subject to profiling;

    - The categories of personal data that were or will be processed as part of the profiling in "Furtherance of Decisions that Produce Legal or Other Similarly Significant Effects";

    - A plain language explanation of the logic used in the profiling process; and

    - Why profiling is relevant to the ultimate decision.

- *Bona Fide Loyalty Programs*: Rule 6.05 would clarify how data right requests impact loyalty programs and the disclosures that are required for those programs. If a consumer exercises their right to delete, and such a deletion would make it impossible for the company to provide program benefits to the consumer, the company would not be obligated to provide the benefit to the consumer. Similarly, if a consumer refuses to consent to the processing of sensitive data necessary for a personalized program benefit, the company would not have to provide that personalized benefit, though it must provide, if available, a non-personalized benefit. Rule 6.05E also requires controllers to disclose certain information with respect to the loyalty program in their privacy notice. These disclosures include the value of the loyalty program benefits.

CONCLUSION

The above highlights scratch the surface of the proposed regulations. The good news is that these are draft regulations, and the AG's Office has invited public comment on not only the proposed regulations themselves but nearly five pages worth of specific

questions regarding the scope and language of the proposed regulations, signaling a demonstrated interest by the AG's Office to invite and consider public comment.

Although the proposed Colorado regulations will not take effect until July 2023, many companies are working now to update their existing programs for CCPA compliance and may want to consider incorporating some of the key Colorado components as they do.