Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 35 • NUMBER 3 • MARCH 2023

Colorado Attorney General's Office Releases Modified Draft Rules for Colorado Privacy Act: Key Takeaways

By Tracy Shapiro, Eddie Holman, Hale Melnick, Clinton P. Oxford and Yeji Kim

The Colorado Attorney General's office has published an updated version of proposed draft rules (modified draft rules)[1] to the Colorado Privacy Act (ColoPA), which revise the initial draft rules it previously issued, based on feedback received during the prior comment period. Notably, the Colorado Attorney General's office explained that it modified some of the rules to facilitate interoperability with the California Consumer Privacy Act (CCPA) as modified by the California Privacy Rights Act (CPRA).

What follows are our high-level takeaways, followed by more in-depth analysis of each point.

- *Privacy Notices*: While the modified draft rules eliminate the requirement for privacy notices to break out personal data collected and shared for each processing purpose, controllers may now have to notify consumers of a change in the notice when they begin sharing personal data with new processors or third parties.

The authors, attorneys with Wilson Sonsini Goodrich & Rosati, may be contacted at tshapiro@wsgr.com, eholman@wsgr.com, hmelnick@wsgr.com, coxford@wsgr.com and yeji.kim@wsgr.com, respectively.

- *Refreshing Consent*: The modified draft rules relax the previous obligation for controllers to refresh previously obtained consent at "regular intervals"; now, controllers must do so only if the consumer has not interacted with them in the past 12 months.

- *Universal Opt-Out Mechanism*: The modified draft rules remove the requirement for controllers to query a "do not sell" list to satisfy their opt-out obligations.

- *Data Protection Assessments*: While the modified draft rules shorten the list of required considerations for data protection assessments, they also add some new ones, such as assessing the operational elements of the processing activity, which may include sources of personal data and technology or processors to be used.

- *Consumer Rights*: The rules on consumer rights now align more closely with the CCPA's. For example, they allow compliance delays if a correction request involves personal data stored in an archived or backup system.

- *Dark Patterns*: The modified draft rules narrow the scope of rules against using dark patterns in user interfaces – the prohibition is specific to user "consent" interfaces, not all user interfaces.

- *Duty of Care*: The modified draft rules introduce new factors, such as applicable industry standards and frameworks, to determine reasonable and appropriate security safeguards.

PRIVACY NOTICES

- *Removed the Disclosure Requirements Centered on "Processing Purposes" (Rule 6.03(A))*: Under the initial draft rules, controllers were required to, among other things, explain why the personal data was reasonably necessary for each processing purpose, an obligation unique in ColoPA. Controllers also had to list the categories of personal data processed for each of the controller's processing purposes, as well as the categories of third parties to whom the controller sells or shares personal data for each processing purpose. The Colorado Attorney General's Office explained that it deleted this requirement in the modified draft rules in response to public comments that it "would be burdensome and would not be interoperable with California Privacy Notice requirements." Instead, the modified draft rules now require that the processing purpose and type of personal data processed be linked in a way that gives consumers a meaningful understanding of how their information will be used.

- *Material Changes in the Privacy Notice (Rule 6.04(B))*: The modified draft rules require controllers to provide notice to consumers when they make substantive or material changes to their privacy notice. The modified draft rules add that substantive or material changes to privacy notices "may include" changes to "the identity of Affiliates, Processors, or Third-Parties Personal Data is shared with." In other words, when a controller begins to share personal data with new parties, controllers may be obligated to notify the consumers of the change. Notably, ColoPA's modified draft rules no longer require controllers to notify consumers 15 calendar days before the material change goes into effect.

REFRESHING CONSENT (RULE 7.08, 7.02(B))

The modified draft rules relax the previous obligation for controllers to refresh previously obtained consent at "regular intervals." Under the new draft, controllers are required to refresh consent only if the consumer has not interacted with the controller in the past 12 months and the controller is either processing (1) sensitive data for a secondary use, or (2) personal data for secondary use involving profiling for a decision that impacts a consumer's legal rights.

The modified draft rules further relax the refreshed consent requirement by adding an exception: controllers need not receive refreshed consent where a consumer has access and ability to update their opt-out preferences at any time through a "user controlled interface," a term that the modified draft rules do not define.

The modified draft rules also remove the separate requirement to renew biometric consent every year.

Lastly, the Colorado Attorney General's office fixed a drafting error by clarifying that controllers must receive ColoPA-compliant consent by January 1, 2024 – not January 1, 2023, as formerly written – to continue to process previously-collected sensitive data.

UNIVERSAL OPT-OUT MECHANISM (UOOM) (RULE 5.04(B), 5.06(A), 5.07(A))

The modified draft rules remove a "do not sell" list as an example of a qualified UOOM specification, which means that controllers would no longer have to query such a list to satisfy their opt-out obligations.

The modified draft rules also clarify that covered entities must honor signals sent from consumers who have adopted a tool (i.e., a browser) that sends opt-out signals by default, but only if the tool was specifically marketed for exercising opt-out rights using UOOM. Previously, covered entities had to honor signals from tools insofar as the tools were prominently marketed for other privacy protective features, even if not specifically for UOOM. However, the modified draft rules state that the tool need not be solely marketed for its UOOM features and can advertise other features alongside them.

The Colorado Attorney General's Office will publish a list of recognized UOOMs that meet all

of the required specifications no later than January 1, 2024, thus voluntarily moving up the April 1, 2024, deadline contemplated by the initial draft rules. Under the modified draft rules, controllers will have six months to recognize UOOMs added to the public list.

DATA PROTECTION ASSESSMENT CONTENT (RULE 8.04)

While the modified draft rules shorten the list of required considerations for Data Protection Assessments, they also add some new ones. For example, the rules no longer require assessing how the personal data processed is adequate, relevant, and limited to what is reasonably necessary in relation to the specified purpose. At the same time, the modified draft rules now obligate controllers to consider the operational elements of the processing activity, which may include sources of personal data, and technology or processors to be used.

CONSUMER RIGHTS

The modified draft rules relating to consumer rights, such as the right of access and right to correction, now more closely align with the CCPA.

- *Right of Access (Rule 4.04)*: The modified draft rules clarify that, in addition to being able to access personal data a controller collects about them, consumers are entitled to access "final Profiling decisions, inferences, derivative data, and other Personal Data created by the Controller which is linked or reasonably linkable to an identified or identifiable individual." This scope tracks closely with the CCPA: in March 2022, the California Office of Attorney General Rob Bonta issued an opinion[2] interpreting the CCPA and took the position that consumers' right to know the specific pieces of personal data includes "internally generated inferences" that businesses hold about the consumer.

- *Right to Correction (Rule 4.05)*: The modified draft rules add that controllers or processors that store personal data on an archived or backup system may delay compliance with the consumer's correction request with respect to an archived or backup system until that system is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose. The language reads almost verbatim from the CCPA Modified Proposed Regulations[3] (Section 7025(c) on delaying compliance with requests to correction).

DARK PATTERNS (RULES 4.02, 7.09)

The modified draft rules remove the specific prohibition against using dark patterns when controllers offer methods for consumers to exercise consumer rights, but add that all disclosures, notifications, and other communications to consumers must be "[s]traightforward and accurate, and must not be written or presented in a way that is unfair, deceptive, false, or misleading."

Moreover, the modified draft rules narrow the scope of rules against using dark patterns in user interfaces – the proposed prohibition is now specific to user "consent" interfaces, not all user interfaces.

Lastly, the draft rules make clear that the principles outlined in Rule 7.09(A) and (B), (i.e., that consent choice options should be presented in a symmetrical way), constitute "factors" in determining a dark pattern, as opposed to individual requirements.

DUTY OF CARE (RULE 6.09)

The modified draft rules explain the security obligations under ColoPA's "duty of care" requirement for controllers in greater detail. For example, the rules add factors to determine what constitutes reasonable and appropriate safeguards, which include, among other things, applicable industry standards and frameworks, sensitivity and amount of personal data, and the risk of harm resulting from unauthorized or unlawful access, use, or degradation of the personal data.

The modified draft rules also introduce more specific security requirements, such as implementing administrative, organizational, and physical safeguards to ensure compliance with covered entities' own data security policies.

CONCLUSION

The Colorado Attorney General's office is tasked with finalizing the rules on technical specifications of UOOMs by July 1, 2023. As a reminder, the ColoPA's effective date and enforcement date also begin on July 1, 2023.

Notes

1. https://coag.gov/app/uploads/2022/12/CPA_Version-2-Proposed-Draft-Regulations-12.21.2022.pdf.
2. https://oag.ca.gov/system/files/opinions/pdfs/20-303.pdf.
3. https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf.