Pre-Rulemaking Considerations for the Colorado Privacy Act

I. Introduction

Colorado enacted the Colorado Privacy Act (CPA) in June of 2021, becoming the third U.S. state to adopt a comprehensive privacy law. The CPA contains express consumer rights, controller and processor obligations, and provisions relating to CPA enforcement and interpretive guidance. The CPA also gives the Colorado Attorney General three distinct categories of rulemaking authority: (1) specific, required authority to draft technical specifications for one or more universal opt-out mechanisms; (2) specific, discretionary authority to create rules governing a process of issuing opinion letters and interpretive guidance; and (3) broader discretionary authority to create rules for the purpose of carrying out the CPA.

The Colorado Department of Law seeks input from interested persons to inform the drafting of effective rules that are consistent with the statute's intent. The Department has developed a public input and outreach strategy to provide a means to contribute feedback, perspective, and expertise in connection with the CPA.

In the first, and current, phase of this strategy we welcome informal input from all members of the public about any aspect of the Department's upcoming rulemaking. Feedback is being collected through a publicly available comment form[1] and a series of informal listening sessions.

This fall, the Department will begin the formal notice-and-comment rulemaking phase by providing a notice of rulemaking and accompanying draft regulations. The notice-and-comment phase will include at least one formal hearing as well as the continued opportunity to submit comments. Formal rulemaking will be governed by the Colorado Administrative Procedures Act (APA)[2] and comments received during the formal rulemaking process will be automatically included in the rulemaking record.

We encourage consumers, regulated entities, and other interested parties to participate in each phase of this process by providing comments and input relevant to any area of the CPA. Comments may address, but are not limited to, areas that need clarification, consumer concerns, anticipated compliance challenges, impacts of the CPA on business or other operations, cost concerns, and any underlying or related research or analyses. In addition, we provide a list of topics and questions below for which we welcome specific feedback. Please note that these topics and questions are not intended to limit input or indicate that the Attorney General is predisposed to any position or action.

II. Principle-guided rulemaking

To enhance the public's understanding of how the Office of the Attorney General will be approaching this rulemaking, we offer five principles to help implement the CPA. In the Department's rules, we seek to:

- **Promote consumer rights**. The rules should protect consumers, understanding that consumers need to understand and exercise the rights granted to them under the law.

[1] Online comment form available at: https://coag.gov/resources/colorado-privacy-act/comments/.
[2] § 24-4-103, C.R.S.

- **Clarify ambiguities**. The rules should clarify the law where necessary to promote compliance and minimize unnecessary disputes.
- **Facilitate efficient and expeditious compliance**. The rules should help controllers and processors comply with the law, by making processes simple and straightforward for consumers, entities, and enforcement agencies.
- **Harmonize**. The rules should facilitate interoperability and help situate the CPA alongside the competing protections and obligations created by other state, national, and international frameworks.
- **Allow for innovation**: The rules should not unduly burden anybody from developing creative, adaptive solutions to address challenges presented by advances in technology.

As the Department considers public input, it will examine how any recommendations and concerns address and advance these key principles.

III. Targeted questions for informal input

Below are topics and questions for which the Department believes informal, pre-rulemaking feedback will be particularly beneficial. The Department hopes to hear from a diverse group of stakeholders to guide the drafting of balanced and impactful regulations.

1. Universal Opt-Out

The CPA contemplates "universal opt-out mechanisms" (UOOMs), technical measures with which consumers may exercise their "right to opt out of the processing of personal data . . . for purposes of targeted advertising or the sale of personal data."[3] The Attorney General is required to "adopt rules that detail the technical specification for one or more" UOOMs, the only specific topic about which the legislation requires us to write rules.[4]

The Department invites feedback about the level of specificity with which to approach this task, as well as input responsive to these specific questions:

- Should the rules point to specific protocols or proposed specifications as exemplars?
- Should the rules discuss specific considerations tailored for different categories of tools that might serve as UOOMs, such as browsers, operating system settings, and browser add-ons, or should our rules remain strictly technology neutral?
- A "technical specification" suggests the need to engage with the technical details of products and services.[5] How can the Department best provide these details while leaving an opportunity for future technical innovation?
- The "rules must not adopt a mechanism that is a default setting, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out of the process of personal data."[6] How should the rules elaborate on this requirement, if at all? Would a tool that

[3] § 6-1-1306(a)(IV)(A), 1306(a)(IV)(B).
[4] § 6-1-1313(2).
[5] *See id.*
[6] § 6-1-1313(2)(c).

is marketed for its privacy features suffice to satisfy this requirement? Would a privacy-focused version of a tool offered in multiple versions suffice?

- The "rules must adopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the United States."[7] What other similar mechanisms have been required?
- The "rules must permit the controller to accurately authenticate the consumer as a resident of this state."[8] What kind of mechanisms should our rules acknowledge to satisfy this requirement?

2. Consent

The CPA requires consent to process consumer data in specific circumstances. For example, "[a] controller shall not process a consumer's sensitive data without first obtaining the consumer's consent or, in the case of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian."[9] "A controller shall not process personal data for purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed, unless the controller first obtains the consumer's consent."[10] Additionally, "[n]otwithstanding a consumer's decision to exercise the right to opt out . . . a controller may enable the consumer to consent, through a web page, application, or similar method, to the processing of the consumer's personal data . . . ."[11] Under the CPA, "'[c]onsent' means a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the process of personal data." "The following does not constitute consent: (a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information; (b) hovering over, muting, pausing, or closing a given piece of content; or (c) agreement obtained through dark patterns."

Receiving information responsive to the following questions will assist the Department in considering regulations regarding consumer consent:

- What is a "clear, affirmative act" in this context?
- What should be required to create "freely given," "specific," or "unambiguous" consent?
- What constitutes "informed" consent?
- Are there specific frameworks, guidance documents, or court decisions from similar legal regimes which help articulate these standards for consent?
- What consent mechanisms allow for adequate consent from a parent or lawful guardian?
- What common methods of obtaining consent currently in use meet the standards set out by the CPA?
- What, if any, limits should be set on methods a controller may use when they request updated consumer consent after a consumer has opted out?

---

[7] § 6-1-1313(2)(e).
[8] § 6-1-1313(2)(f).
[9] § 6-1-1308(7).
[10] § 6-1-1308(4).
[11] § 6-1-1306(1)(a)(IV)(C).

3. Dark Patterns

As discussed above, the CPA expressly states that agreement obtained using "dark patterns" does not constitute consent.[12] Dark patterns are defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice."[13] Comments in response to the following questions will assist the Department in considering regulations relating to dark patterns under the CPA:

- What standards or principles would best guide design choice to help avoid the inadvertent use of dark patterns?
- Should the rules outline specific types of dark patterns which are prohibited?
- Are there specific frameworks or tools already in existence that help identify dark patterns?
- What user interface design choices currently in use may subvert or impair consumer autonomy or decision-making, for example by manipulating, confusing, misdirecting or tricking consumers? Which ones may impact consumer choice, for example by causing an asymmetry of information between consumers and businesses?
- What recent research best demonstrates the impact of specific dark patterns or design choices on consumers?

4. Data Protection Assessments (DPA)

The CPA provides that a "controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data acquired on or after the effective date of [the CPA] that present a heightened risk of harm to a consumer"[14] Activities that present a "heightened risk of harm to a consumer" include processing for the purpose of targeted advertising, selling personal data, processing sensitive data, and processing for the purpose of profiling that creates a reasonably foreseeable risk of unfairness, injury, or offensive intrusion of privacy.[15] The CPA further obligates Controllers to provide those DPAs to the Attorney General upon request.[16]

Comments in response to the following questions will assist the Department in considering regulations relating to the CPA's data protection assessment (DPA) requirement:

- In what circumstances should the Department request a DPA?
- How much and what type of guidance should the rules provide with respect to form and content of DPAs?
- Should DPAs follow any existing model such as the EU model, enterprise risk management approaches, or environment impact statement model?

---

[12] § 1303(5)(c).
[13] § 6-1-1303(9).
[14] § 6-1-1309(1).
[15] § 6-1-1309(2)(a)(I)-(III).
[16] § 6-1-1309(4).

- Should Colorado consider DPAs to be compliant when they have been conducted for and are compliant with another regime? If so, which regimes?
- What information should DPAs contain with respect to processing for the purpose of profiling?
- The CPA allows for a single data protection assessment to address "a comparable set of processing operations that include similar activities." [17] What makes processing operations comparable? What makes activities similar?

5. Profiling and "Legal or Similarly Significant Effects"

The CPA authorizes Colorado consumers to "opt out of . . . profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."[18] Profiling consists of "any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, locations, or movements."[19] Decisions that produce legal or similarly significant effects concerning a consumer are those that "result[] in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services."[20]

Comments in response to the following questions will assist the Department in considering regulations concerning decisions that produce legal or similarly significant effects under the CPA:

- What type of transparency would meaningfully allow consumers to understand the automated processing of their personal data such that they can make informed opt out decisions? Should this vary by the type of automated decision in question?
- Are there individual legal or civil rights concerns regarding automated profiling that should be specifically addressed in the rules?
- Are there specific applications of "profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer" which may warrant additional consideration or specific rules?"
- What are the potential negative impacts of immediately opting a consumer out of profiling that produces legal or similarly significant effects upon request? What appropriate mitigation might exist?
- What, if any, special considerations may apply to opting out of profiling in the specific areas outlined by the statute (e.g. "the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.")?
- What areas of overlap between the definitions of profiling and decisions that produce legal or other significant effects may be inconsistent or require clarification?
- What has been most effective in similar legal regimes concerning profiling or automated decision making?

[17] § 6-1-1309(5).
[18] § 6-1-1306(a)(I)(c).
[19] § 6-1-1303(20).
[20] § 6-1-1303(10).

- How should this language apply to "partial" automated decisions that involve human oversight once the automated decision is made?

6. Opinion Letters and Interpretive Guidance

The CPA authorizes the Attorney General to adopt rules governing a process to issue opinion letters and interpretive guidance by January 1, 2025.[21] Comments in response to the following questions would assist the Attorney General in determining a framework for an interpretive guidance process:

- What type of interpretive guidance should the rules provide, and what should the process of obtaining interpretive guidance to look like?
- Can an interpretive guidance process could be abused and if so, how?
- Is there an existing interpretive guidance process prescribed by a separate statutory regime that is effective? If so, which one?
- What level and form of disclosure or public notification of such opinion letters or guidance is appropriate to maximize compliance?

7. Offline and Off-Web Collection of Data

Many businesses and non-profits collect personal information through non-electronic methods such as filling out a rental form, signing a petition on a sidewalk, or buying a magazine subscription. Though this information may be collected on paper, it may later be entered into a digital data base.

Comments in response to the following questions will assist the Department in considering regulations to clarify how consumer rights and controller obligations apply to offline collection and use of personal data.

- How should the rules address the offline collection of data?
- What are the challenges to fulfilling controller obligations when conducting offline information collection and processing?
- What are the challenges to maintaining consumer privacy preferences in offline interactions?
- Should the UOOM technical specifications cover personal data collected offline or off-web? If so, how can they do so most effectively?

8. Protecting Coloradans in a National and Global Economy

The Attorney General undertakes this rulemaking as an official of the State of Colorado entrusted with protecting the people of this state. At the same time, the CPA and the rules protect Coloradans participating in national and global markets and networks. Similarly, the CPA and the rules coexist with similar laws in other local, state, national, foreign, and international jurisdictions.

The Department invites feedback and information to assist in rulemaking in these complex contexts, such as:

- What does the CPA do differently from laws in other jurisdictions?
- What does the CPA do the same as law in other jurisdictions?

[21] § 6-1-1313(3).

- What privacy interests do the people of Colorado tend to emphasize more than or differently than the privacy interests of people elsewhere?
- Where does the CPA overlap with laws of other jurisdictions in ways that should be considered in CPA rulemaking? How can the rules address these overlaps in a way that would best avoid consumer confusion and compliance conflicts?

9. Additional Topics+

The Department invites any additional input relating to the CPA that should be considered during the rulemaking process. This may include, but is not limited to, areas that may need further guidance or clarity, areas that may be confusing to consumers, consumer rights request or compliance obstacles, the impact of the law on business operations, and any information, analysis, or examples that can further illustrate or support any comments or positions.

IV. Further information

The CPA comment portal is available at https://coag.gov/resources/colorado-privacy-act/comments/. The Department of the Attorney General further encourages members of the public to visit coag.gov/CPA to join the CPA mailing list and to find additional information about the CPA.