Computer & Communications Industry Association
Tech Advocacy Since 1972

November 7, 2022

Via Electronic Portal

Office of the Attorney General
Colorado Department of Law
Ralph L. Carr Judicial Building
1300 Broadway, 10th Floor
Denver, CO 80203

Re: Comments for Proposed Rulemaking Pursuant to the Colorado Privacy Act of 2021

The Computer & Communications Industry Association ("CCIA")[1] is pleased to respond to the Colorado Department of Law's (the "Department") Notice of Proposed Rulemaking on the Draft Rulemaking (the "draft Rules") governing the implementation of the Colorado Privacy Act (the "CPA").

INTRODUCTION

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. We support and appreciate the Department's efforts to adopt and implement privacy regulations that will guide businesses and protect consumers. These comments focus on the provisions in the draft Rules that warrant revision. The aim of these suggestions is manyfold. First, to ensure that the final Rules are reflective of the mandates stated in the CPA. Secondly, the final Rules are feasible to implement in a timely and clear manner. And third, the final Rules allow flexibility in order to not inhibit innovation.

CCIA's suggested amendments to the draft Rules are set forth in **Attachment A**.

I. DEFINITIONS

A. "Automated Processing" – Rule 2.01

The draft Rules define "automated processing" far too broadly as to include *any* processing of personal data that is automated through "the use of computers, computer programs

[1] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

or software, or other digital technology." The draft Rules proposed definition would apply to calculators, spreadsheets, emails, and calendar software—creating costly regulatory burdens by potentially requiring notice, opt-out, consent, and data protection assessments (DPA) for novel technology. For example, if a company logs a rental applicant's rental history into a spreadsheet and sorts it by year, this would fall under the definitions of automated processing, and profiling, in furtherance of decisions that produce legal or similarly significant effects.

To help remedy this overbreadth, CCIA suggests the final Rules incorporate the concept of materiality for any requirements around profiling. For the compliance obligations to take effect, automated processing should be material to the decision that produces legal or similarly significant effects or material to the risks that prompt DPAs.

B. "Biometric Data" and "Biometric Identifiers" – Rule 2.01

The draft Rules define "biometric data" in a needlessly complex manner that involves a separate sub-definition for "biometric identifiers"—going beyond the core concerns identified in the CPA. Problematically, the definition of "biometric identifiers" is overbroad and could include common data types such as photographs, video, and audio that are not used for identification purposes. Accordingly, CCIA recommends defining "biometric data" in accordance with emerging U.S. state comprehensive privacy laws such as those in Connecticut and Virginia, substituting the defined term "biometric data" for all relevant obligations (as opposed to "biometric identifiers"), and creating a specific carveout for the Health Insurance Portability and Accountability Act.[2]

C. "Intimate Rule" – Rule 2.01

The proposed definition of an "intimate image" is problematic for it invites, amongst other challenges, subjective considerations that make it difficult to operationalize without creating legal risk for a business. Specifically, the inclusion of "[a] part of the body, if revealed publicly, the subject would find sensitive or offensive based on their religious belief," introduces a level of subjectivity that makes compliance difficult, given the wide variance in modesty standards across religions. CCIA requests the Department modify the final Rules language to

[2] Connecticut Data Privacy Act, P.A. 22-15 Section 1(3), https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF; Virginia Consumer Data Protection Act, S.B. 1392 Section 59.1-571, https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf.

account for this concern and avoid creating this unnecessary risk to businesses.

II. CONSUMER DISCLOSURES

A. Requirements for Disclosures, Notifications, and Other Communications to Consumers – Rule 3.02(A)(5)

As written, the draft Rules do not provide sufficient language specifying the scope of the readability requirements for devices. CCIA suggests the Department clarify that this does not apply to headless devices with which consumers are not expected to interact with by reading—including headless devices and video platforms.

III. CONSUMER PERSONAL DATA RIGHT

A. Right to Opt-Out – Rule 4.03

The draft Rules on the general right to opt-out conflict with the CPA's intent and creates regulatory burdens that may prevent benefits from reaching consumers.

The CPA expressly removes the right to opt-out of profiling from under the general rule of providing the opt-out.[3] The draft Rules, however, eliminate the distinction between the ability to opt-out of profiling with targeted advertisement and the sale of personal data, to the extent it puts all three in the definition of "Opt-out Purposes." Profiling opt-outs are often focused only on specific services that may eventually have decisions with legal or similarly significant effects. Due to its highly contextual nature, profiling opt-outs tend to be located in the specific user experience (UX) and not generally in the privacy notice. This obfuscation may also confuse consumers on what decisions they are actually opting-out to. CCIA recommends the final Rules restore this distinction to reflect the statute's intent.

The draft Rules' broad framing is also overly restrictive and imposes new burdensome requirements upon businesses. The draft Rules, as written, would require the right to opt-out of profiling to be available to customers at or before the time of collection. This language would force companies to provide an opt-out before any decision is actually made, meaning that a consumer may not receive the benefits created by automated decisions. The EU General Data Protection Regulation, for example, grants individuals the right to request a review of automated

[3] Colorado Privacy Act, § 6-1-1306, (1)(a)(III,) https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

decisions if the individuals feel they are being harmed.[4] However, this right is only available *after* a decision is made. The draft Rules could also create a worse experience for consumers when companies in an attempt to comply with burdensome requirements are forced to adopt slow, and costly human elements for decisions. All of this, again, without any real harm. CCIA recommends the final Rules reflect the GDPR approach and permit individuals to opt-out once a decision is made, which could then trigger a right to a human review.

The draft Rules also invite unnecessary confusion in draft Rule 4.03(B)(1) by requiring multiple locations—inside privacy notice, outside privacy notice—for opting out of profiling. The final Rules should seek to help consumers understand where they can find information on rights through a centralized location, enabling companies to determine whether additional links are needed on a case-by-case basis. For that reason, CCIA recommends the Department allow businesses the option of presenting a single privacy link that captures all privacy controls for consumers. This will reduce the burden on how consumers exercise their privacy choices and minimize clutter and confusion on web pages with multiple links to multiple opt-out landing pages. To that end, this rule should permit link text that provides a clear understanding of this broader purpose, such as "Your Privacy Choices."

CCIA also recommends that the Department remove the reference to the "app store" in draft Rule 4.03(B)(1) as the consumer's data is likely not collected at this stage. Instead, the final Rule should permit a business to place the link in the application after the consumer has downloaded it.

B. Right of Access – Rule 4.04(A)

The right to access, as outlined in the draft Rules, would impose contradictory compliance requirements on businesses. Controllers would be required to provide "without limitation, any Personal Data" they obtained, but it must be both "understandable to the Controller's target audiences" and avoid "incomprehensible or unexplained internal codes and identifiers." These opposing obligations create unnecessary friction for businesses and consumers, resulting in potentially longer response times to consumers. The current language

[4] *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Council Directive 95/46/EC (General Data Protection Regulation), 26 O.J. (L 119), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

also introduces legal risk if a Controller's responses are found to not be understandable by segments of the business' large and diverse target audience. The proposed language needs to be updated to allow businesses the necessary flexibility to operationalize these requirements. As such, CCIA's suggested amendments to the draft Rules seek to limit the requirements around practicality, including refining the portability requirements in draft Rule 4.04(B) to a feasibility standard whereby Controllers are not required to provide services beyond what is technically possible.

C. Right to Correction – Rule 4.05(A)

As written, the draft Rules require Controllers to correct personal data "across all data flows and repositories." This expanded definition could affect archival and backup systems, imposing a significant burden on businesses while yielding little benefit to consumers. CCIA suggests that the language be modified to account for the importance of proportionality.

D. Right to Deletion – Rule 4.06(D)

The draft Rules unnecessarily require businesses to identify which categories of data are not deleted for each consumer deletion request. This new burdensome requirement is also not offset by any countervailing benefit to consumers. To avoid this burden, CCIA recommends that it should be sufficient for businesses to disclose the categories of data that it does not delete.

E. Right to Data Portability – Rule 4.07(B)

Draft rule 4.07(B) helpfully clarifies that the portability right excludes disclosure that would infringe on trade secrets. However, the exception in draft Rule 4.07(B)(1) is inconsistent with that protection to the extent it carves our inferences from algorithms without any limitation. For instance, a business might use machine learning (ML) to create customer profiles. These profiles result from substantial investment and research and development. If this process were to be subject to the portability right, it would convey an unfair economic advantage to a competitor. If this exception is retained, CCIA recommends that it should exclude situations where the algorithm can be reverse-engineered from the inferences.

IV. UNIVERSAL OPT-OUT MECHANISMS

A. Rights Exercised – Rule 5.02(C)

The draft Rules refer to permitting the UOOM to allow consumers the ability to opt-out of processing for a "specific purpose." CCIA suggests the Department clarify that this refers to the specific opt-outs for either targeted ads or the sale of personal data. The draft Rules should not otherwise permit UOOMs to provide opt-outs for other, more granular purposes would be too burdensome for businesses to receive UOOMs that convey numerous types of opt-outs.

B. Default Settings – Rule 5.04(B)

Currently, the draft Rules conflict with the statutory requirements concerning default settings and informed consent. Per the CPA, the UOOM may not be a default setting and must clearly represent the consumer's affirmative, freely given, and unambiguous choice to opt-out of the processing of personal data. Furthermore, draft Rule 7.03(C)(2)(a) defines freely-given consent as valid only if it is not "bundled with other terms and conditions."

Simply choosing a privacy-focused application or browser is an isolated action, it does not translate to or constitute one's affirmative acknowledgment and the decision to opt-out of ads targeted to their preference. A consumer who buys a privacy-enhancing product may just want to avoid cookie tracking or other data sharing, and not opt-out of ads targeted to their preferences. Absent specific marketing on these opt-out functions, a consumer cannot be deemed to have freely and unambiguously consented to activate the UOOM. The proposed language would mean that the consent to the UOOM is bundled with all of the other privacy-enhancing features of the device. This default, implied opt-out would lead to a significant number of erroneous opt-out signals—opting out of certain forms of processing can impact a consumer's UX and access to certain features. As a result, consumers may be confused and annoyed if their services are interrupted due to an erroneous opt-out.

CCIA suggests the Department strike draft Rule 5.04(B) to avoid creating compliance challenges for Controllers and significant confusion about what constitutes a UOOM.

C. Technical Specification – Rule 5.06

For UOOMs that are received on company websites, the Department should confirm that HTTP should be the only format permitted for UOOMs that are sent from a browser or

application. Permitting other formats creates greater friction for companies to recognize users' opt-out choices and creates further consent fatigue for customers. And at a device level—where the UOOM signal would typically arrive in the HTTP header from each app communicating with the relevant servers—should businesses rely on a single app on a given device to convey the UOOM signal for the device as a whole? Different apps cannot send distinct signals on a single device as such, CCIA suggests the Department clarify the intent around this requirement.

CCIA recommends the final Rules be modified to ensure the scope of permissible UOOMs is not expanded to include requiring a business to ping a "do not sell" list. From a technical perspective, a business will face a significant burden to build a mechanism that can send outbound queries to honor opt-out requests when compared to receiving an inbound opt-out signal. This burden is compounded to the extent that Colorado would require a company to ping multiple "do not sell" lists. From a consumer benefit perspective, querying a "do not sell" list would add latency to online experiences. From an effectiveness perspective, depending on the format of the list—user names, addresses, emails, or device IDs—businesses may not be able to match a consumer accessing a website to a consumer on the "do not sell" list. To the extent the final Rules do permit "do not sell" lists, the final Rules would have to provide clear guidance on a standardized list format, encryption standard, access application programming interface (API), and service level agreements for latency and data accuracy. Even so, successful user matches still could not be expected to reach 100%. Data normalization, even when applied consistently on both sides, cannot account for all differences in the stored data.

CCIA recommends the Department include a security standard for UOOMs and a carve-out permitting businesses not to honor opt-outs that were submitted fraudulently. The standards should enable businesses to immediately recognize whether a given UOOM is legitimate within the meaning of the law. Businesses cannot feasibly receive and recognize just any hypothetical opt-out signal that may be transmitted by any conceivable source. Otherwise, there is a risk that bots could send a high volume of opt-outs through UOOMs and overwhelm businesses' opt-out systems. A bad actor could also send false opt-out signals or use the signals to gain unauthorized access to a receiving company's systems or consumer data.

D. Systems for Recognizing UOOMs – Rule 5.07

The public list of UOOMs will reduce uncertainty and implementation burdens for businesses as long as the list is limited to a relatively small number and is updated only on a regular cadence, such as once per year. CCIA recommends the draft Rules be modified to provide Controllers with at least six months to implement the acceptance of recognized UOOMs, given the complexity of implementing multiple UOOMs across various web surfaces simultaneously. However, if the final Rules permit multiple formats of UOOMs, Controllers will need more than six months to account for significant additional technical work.

CCIA also requests the Department to formally confirm whether the Global Privacy Control (GPC) is an acceptable UOOM for purposes of the CPA.

E. Obligations on Controllers – Rule 5.08 (A)

The draft Rules as written would require the Controller to apply the opt-out request at the consumer level "if known." However, some Controllers consist of multiple businesses with separate customer accounts (like Facebook.com and WhatsApp). Consumers would be confused if their targeted ads preference for one service and it automatically carries over to the other, in particular where a consumer would prefer different settings for different accounts. And the draft Rules in(A)(2) create a technically infeasible requirement to persistently honor a consumer's opt-out request from a UOOM if the consumer is not authenticated. CCIA suggests the Department clarify that a business should continue to honor a UOOM to the extent it can continue to recognize the authenticated consumer.

F. Consent after Universal Opt-Out – Rule 5.09(B)

The Department should clarify the language here to adopt more flexibility and innovation. Specifically, if the UOOM technical specifications enable it to indicate to the consumer that it has turned the UOOM signal *off*, then the Controller should be able to interpret that as an opt-in to the extent that the consumer had previously opted out with that same Controller with that same UOOM signal.

V. DUTY OF CONTROLLERS

A. Privacy Notice Content – Rule 6.03

The text in draft Rule 6.03(A)(1) creates a heavy obligation for Controllers to provide information "for each Processing purpose." CCIA is concerned that requiring Controllers to organize a privacy notice by purpose would be unduly burdensome, particularly for those who already use a global privacy notice across multiple jurisdictions. For consistency, the Department can look at the approach taken in other state privacy laws, notably the California Privacy Rights Act which focuses on the disclosure of data categories rather than processing purposes. Furthermore, it is unclear whether this obligation would provide a material benefit to consumers while imposing a clear cost—an increase in the length and complexity of existing privacy notices for consumers. CCIA recommends the final Rule be modified to ensure that a business is not required to organize privacy notices by purpose.

The draft Rules also require that every category of personal data for a Controller processes the data of a child. To avoid this unnecessary burden, CCIA recommends that the draft Rules permit companies to be able to take appropriate care regarding child data by either assuming the responsibility for processing child data for every category or not knowingly processing child data.

The ambiguous language in draft Rule 6.03(A)(5) could conflict with the requirements for the Controller's duty regarding sensitive data. Draft Rule 6.10(C) requires a Controller to include information about "Sensitive Data Inferences" in its privacy notice only "if a Controller *will* delete [such data] within 12 hours." Conversely, draft Rule 6.03 would require a Controller to include such information in its privacy notice "*if*" it will delete such data within 12 hours. As such, CCIA recommends revising draft Rule 6.03 to avoid this conflict and compliance for data that is deleted within 12 hours.

B. Changes to a Privacy Notice – Rule 6.04

The requirement to notify consumers of substantive or material changes to their privacy notice 15 days before the change goes into effect would be unduly burdensome. Companies operating in multiple jurisdictions may need to update their global privacy notices quickly based on changes in local law. This new requirement for Controllers provides no corresponding benefit

to consumers and defeats Colorado's stated goals of promoting interoperability and harmonization. CCIA recommends the Department delete this language.

C. Loyalty Programs – Rule 6.05

As written, draft Rule 6.05(A) prohibits a Controller from increasing the cost of or decreasing the availability of a product or service based solely on a consumer's exercise of data. This restriction conflicts with draft Rules 6.05(B)-(D) and (F). The latter section's language illustrates the understanding that businesses may need to increase costs or decrease the availability of a product or service as a result of a consumer's decision to exercise a data right. For instance, ad-supported tiers of services are widely understood and accepted in the video streaming industry. If a consumer opts out of targeted advertising, the business should be allowed to make up the revenue difference by charging more for the service. To resolve the conflict, CCIA suggests the final Rules instead require that the price or service differential be reasonably related to the value of the consumer's data—consistent with the CPA.

D. Secondary Use – Rule 6.08

The vague language in draft Rule 6.04(C) invites unnecessary confusion, creating legal risk for Controllers. Specifically, draft Rule 6.04(C) is not compatible with the language in Rule 6.08(B) unless the term "secondary use" suddenly refers to a purpose that is not reasonably necessary to or not compatible with the processing purpose specified at collection. Draft Rule 6.08(B) imposes an additional consent requirement for processing for a secondary use if that secondary use is not necessary to or compatible with the specified purpose. However, the language in 6.04(C) is broader, requiring consent for any secondary use, even if disclosed in the privacy notice. Draft Rule 6.08(B) imposes a more reasonable standard and aligns more closely with draft Rule 7.02(A)(4).

CCIA is also concerned that the multi-factor nature of the test for whether a processing purpose is "secondary" will create legal risk if a company's application of the test differs from the Colorado Attorney General's expectations. This proposed test includes several factors, none of which is dispositive or designated as being of greater import, so reasonable individuals may reach different conclusions about whether a purpose is "secondary." CCIA suggests the Department clarify that businesses should not have to go back to the customer for

every secondary use so long as those uses are compatible with the original purpose for which the customer provided the data.

E. Duty Regarding Sensitive Data – Rule 6.10

CCIA recommends changing references of "Personal Data and any Sensitive Data Inferences" to simply "Sensitive Data" and/or "Sensitive Data Inferences." As written, the draft Rule will create legal compliance challenges because it applies to the personal data upon which sensitive and personal data is based, which is vague and unclear. CCIA also suggests the exception for consent to sensitive and personal data to be modified to cover data that is permanently deleted within *24 hours* rather than *12 hours*, which will reduce the burden on business and account for variance in monitoring that occurs during the day.

CCIA suggests the Department ensure that businesses do not have to go back to the customer for every secondary use so long as those uses are compatible with the original purpose for which the customer provided the data.

F. Documentation Concerning Duties of Controllers – Rule 6.11

The draft Rule requirements for Controllers to maintain records of all Data Rights requests for at least two years is an unnecessary and disproportionate risk for businesses. The volume of store records could create a large and ever-expanding vulnerability for Controllers, increasing the cost of maintaining reasonable security measures for the data and the risk of cyberattacks that involve it. The draft Rule also requires a new Controller to continue to recognize previously-exercised Data Rights, which increases the due diligence burden and legal risks associated with acquisitions, especially for the acquisition of companies with immature privacy compliance programs. CCIA recommends the Department revise the final Rules to alleviate this burdensome requirement in light of these concerns.

VI. CONSENT

A. Requirements for Valid Consent – Rule 7.03

CCIA recommends the final Rules clarify that a consumer consents through affirmative action when they knowingly and intentionally disclose personal data in certain settings. For instance, a consumer who intentionally submits sensitive demographic data (such as citizenship

status or religious affiliation) while completing an online form should be deemed to have consented to collecting and processing that demographic data. The Department should clarify that the use of *pre-selected* opt-out options, which would direct consumer decision-making toward one or more pre-set outcomes, is prohibited. To the extent some pre-selected options are permitted, vendors should not offer multiple versions of the same tool—consumers should not be faced with consent interfaces that have all of the opt-outs preselected and another allowing consumers to select opt-out options themselves. Effectively, directing consumer decision-making toward one or more pre-set outcomes undermines the concept of affirmative choice.

Draft Rule 7.03(C)(a) provides that consent is not freely given when it is bundled with other terms and conditions. CCIA recommends this language be modified to permit an exception where the business provides an option to provide more granular consent, allowing for innovative flexibility that would yield further benefits for consumers.

Draft Rule 7.03 (E) is overly broad and would apply in a wide range of scenarios including where a consumer wants to re-opt-in to ads targeted to their preferences. This would impose a significant burden on companies and confusion for consumers to the extent it would require detailed disclosures whenever a consumer chooses to opt-in. Instead, the consumer should be able to click a check box or toggle to provide consent. The language around "informed consent" should not limit a company from collecting or processing data only for functions or programs that exist at the time of the consent. Customers benefit from the speedy launch of new experiences and features, which they would be denied if the company had to restart the consent process for every innovation. CCIA proposes the Department strike this requirement in its entirety or limit it to certain high-risk situations.

While the CPA's text prohibits the use of dark patterns to obtain consent, the draft Rules broadly state that dark patterns are prohibited in all circumstances. This ambiguity fails to provide Controllers with the requisite guidance and the proposed language seemingly goes beyond the scope of the statute. CCIA requests the Department *make clear* that the final Rules should not exceed the scope of the CPA.

B. Consent for Children – Rule 7.06(A)

CCIA recommends the Department remove or clarify the requirement that a Controller verifies a Consumer's age if it has "a website or business directed to Children or has actual

knowledge" it collects a child's personal data. The Rules should not require the collection of additional sensitive data such as birth dates to obtain consent in contexts where collecting age is not necessary to obtain verifiable parental consent. Alternatively, CCIA asks the Department to provide more specificity about what "commercially reasonable steps" are required to verify a consumer's age. The requirements for consent for children should be aligned with federal requirements under Children's Online Privacy Protection Act.

C. Refusing or Withdrawing Consent – Rule 7.07(A) and (E)

CCIA recommends draft Rule 7.07(A) be modified to recognize situations where a business may surface a consent request when a consumer first visits a website, but then not continue to surface the same interface every time afterward. As written, the draft Rules could mandate this tedious requirement. Instead, the number of steps required to revoke consent should be compared to the number of steps it would take the consumer to affirmatively give consent at the particular point in time that the consumer wants to make that choice.

Draft Rule 7.07(E) as written unnecessarily burdens businesses and disrupts the consumer experience. It requires a business to surface deletion instructions each time a consumer modified a processing preference—such as opting in or out of targeted advertisements. CCIA recommends the Department clarify that it should be sufficient for the business to disclose in its privacy notice how a consumer can exercise their deletion right.

D. Refreshing Consent – Rule 7.08(A)

The draft Rules require Controllers to obtain "refreshed consent" at least annually for processing sensitive data and "at regular intervals" for all other data processing that requires consent. The draft Rules further mandate Controllers obtain consent for processing inferences derived from sensitive data unless the Controllers adhere to specific use cases for such inferences. Both of these obligations create new requirements that conflict with the plain text of the CPA.

The draft Rules, as written, define consent in an overly broad way to include a scenario where a consumer opts-in to certain processing activities only after initially opting-out. These changes do not appear to be targeted at any consumer benefit, as a business could process data without initially obtaining consent but would then need to obtain repeated consent only after the

consumer has opted back in. This adds a significant burden for consumers, who already experience "consent fatigue" due to the overwhelming number of consents they are asked for online.[5] The proposed language could also conflict with draft Rule 7.09(B)(6) to the extent that it would unnecessarily interrupt and intrude on a consumer's expected interaction with a website or application, especially given that Controllers are already required to allow consumers to revoke consent as easily as they affirmatively provide it. The regular interval requirement is inconsistent with other state laws and undermines Colorado's interoperability and harmonization goals. The requirement creates risk for businesses that will have to delete customer resources if, for some reason, the customer does not respond to the business' consent outreach. And this requirement could potentially require businesses to collect more information from customers for the sole purpose of ensuring they have a way to communicate consent requests.

CCIA recommends the requirement for Controllers to refresh consent at regular intervals be deleted. Alternatively, CCIA recommends that the final Rule modify this requirement to permit continued consumer engagement as a form of consent, or at a minimum, not requiring recurring consent within a period shorter than 18 months.

E. User Interface Design, Choice, Architecture, and Dark Patterns – Rule 7.09

The draft Rule introduces an ambiguous standard for an acceptable interface design or choice architecture that makes it excessively difficult to operationalize without creating legal risk. Controllers would have to determine what rises to the level of a "substantial effect" or impairment of user choice. The listed design principles are also problematic for they adopt subjective standards by requiring Controllers to asses and avoid the use of "emotionally manipulative language" and consider the "vulnerabilities or unique characteristics of the target audience" for a product, service, or website. CCIA strongly advises the Department to modify the final Rules to reflect a more objective and practical standard.

The proposed language in draft Rule 7.09(B)(4) is incompatible with the text of the CPA. The CPA provides consumers with the right to opt-out out, creating a default state—consumers are opted-out. CCIA recommends this requirement be deleted.

---

[5] Brooke Auxier,et al, Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Data, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (Pew Research found that 25% of Americans say they are asked to agree to a privacy policy "almost daily.")

The example in draft Rule 7.09(B)(9) is overly prescriptive for businesses and impractical given the nature of digital surfaces. For instance, a business may place a link seeking consent in the footer of a website homepage through a single click. Yet, since an application does not contain the same type of footer, the business may need to place the same link through the settings options, which would necessitate more than one click. CCIA requests the Department to delete this example.

VII. DATA PROTECTION ASSESSMENTS

A. Data Protection Assessment Content – Rule 8.04

The proposed language on the requirements for DPAs is overly broad, making it excessively burdensome for Controllers to comply with these important assessments. The draft Rules go beyond the general requirement of providing information at the categorical level and instead, mandate overly descriptive requirements such as listing the specific types of personal data to be collected, their sources, and the names of recipients. It is unclear why providing operational details such as planned collection processes or technology used is necessary, given the serious risk it poses to stifling innovation by creating a procedural impediment to updating these processes and/or technologies. The requirement to document alternative activities may also disincentive technological progress—Controllers may hesitate to evaluate technologies that could mitigate processing for the fear that if the Controller decides not to employ the alternative, they may have to justify the decision to Colorado Attorney General. CCIA suggests the Department modify these requirements to address these concerns.

VIII. PROFILING

A. Scope – Rule 9.02(D)

CCIA strongly recommends that "Automated Processing" should ***not*** include "Human Involved Automated Processing" (HIAP). HIAP is considered those decisions where "human involvement in the Processing includes meaningful consideration of available data used in the Processing as well as the authority to change or influence the outcome of the Processing." The level of human review is so significant that this should not be considered "automated" processing anymore, adopting the current interpretation could also cause a lot of confusion. This is especially concerning given that the draft Rules are creating obligations for HIAP as well. And

considering the extremely broad concept of "Automated Processing," it could be read to strictly incorporate anything related to a computer, such as if a person is using a spreadsheet and makes a relevant decision. CCIA's suggestions in Attachment A align with other privacy laws like those in Connecticut and the GDPR.

B. Opt-Out Transparency – Rule 9.03

The "serving ads" language in draft Rule 9.03(A)(5) directly contradicts the CPA, which states a decision that produces legal or similarly significant effects means "a decision that results in the provision or denial" of certain services. The draft Rules should not consider serving advertisements to have a "legal or similarly significant effect" because ads do not impact access to the product or service. Moreover, the draft Rules as written invite significant confusion by mixing opt-out for targeted advertisements and profiling if included in the same manner, especially considering that customers will already have an opt-out for targeted advertising. Accordingly, CCIA proposes removing serving ads to align the final Rules with the text of the CPA and emerging U.S. state comprehensive privacy laws.

CCIA recommends the protection in draft Rule 9.03(B) be expanded beyond *only* trade secrets to include "proprietary information." This protection should also be applied to the DPAs as described in draft Rule 9.06(F) as well.

Draft Rules 9.03-9.05 require Controllers to provide consumers with an overly prescriptive explanation of the logic involved in the profiling process. The draft Rules run the risk of imposing obligations that conflict with the business's intellectual property, trade secrets, and other legal rights. To provide information about the logic involved, businesses should be permitted to describe the general criteria or categories of inputs used in reaching a decision. For example, if a rental company considers certain personal information when evaluating a housing application, those categories of information could be described. A more detailed description of any complex algorithms involved in automated decision-making will not provide the average consumer with meaningful information on the logic involved in the processing. CCIA suggests the Department clarify that a plain-language explanation of the logic used in the profiling process is sufficient.

C. Opting Out of Profiling in Furtherance of Decisions That Produce Legal or Similarly Significant Effects Concerning a Consumer – Rule 9.04(C)

The final Rules should not impose any further burdens on HIAP. The definition of profiling is already overly broad, and "automated processing" equally could apply to any trivial action done with a computer and involving customer data–simple use of a spreadsheet. By creating this requirement, the Department could be putting in scope decisions that were entirely made by humans if they only used a computer. If the idea is to ensure fairness, the final Rule should not extend to decisions where humans assess the information and made a decision.
A Controller should be able to satisfy the requirements in draft Rule 9.04(C) through a publicly available notice on a website, instead of individual responses to consumers. This approach would reduce the burden on companies seeking to comply with the Rules and provide consumers with sufficient enough information to meet transparency needs as well. A Controller could post language that outlines its policy on declining opt-out requests in cases of human-involved automated processing we will decline opt-out requests and provide more information on its HIAP. Instead, the Department could encourage businesses to find more efficient ways to provide information to consumers who are declining to opt-out of human-involved automated processing. CCIA strongly advises against including HIAP in the scope of this final Rule because the decision is an affirmative action made by a human, not automated.

D. Data Protection Assessments for Profiling – Rule 9.06

Draft Rule 9.06(A) newly requires a DPA if the profiling presents a reasonably foreseeable risk of various listed harms. To maintain parity with other privacy regimes, CCIA recommends that a DPA should be required only where risk is "likely to result", as is required under the GDPR, rather than "reasonably foreseeable."

CCIA recommends that the language in draft Rule 9.06(B) be modified to ensure regulation of profiling and exclude human-involved reviews for the aforementioned reasons.

CCIA is concerned that the language in draft Rule 9.06(E) defining a "Substantial Injury to Consumers" does not appropriately target risk. Specifically, the section as written could unnecessarily require Controllers to conduct profiling DPAs even if their use case presents a low risk. And the CPA's texts appear to require DPAs only when profiling takes place—but it does not need to be in furtherance of legal or similar decisions—and there is a reasonably foreseeable

risk of another substantial injury to consumers (among other things). However, the draft Rule's definition expands to include "small harm to a large number of consumers" to create a requirement that does not appropriately balance the risk of harm against the benefits of technology. For example, does a GPS taking consumers on a route that is longer by a minute constitute a "small harm to a large number of consumers"? It is unclear if the legislators intend for that low-risk outcome to trigger a DPA, given the risk it could substantially slow down business. To avoid invoking the onerous obligations of the DPAs, CCIA encourages the Department to reserve this requirement for true, high-risk scenarios where heightened oversight is needed.

Draft Rule 9.06(F) should be modified to permit a Controller to rely on a DPA prepared in connection with one jurisdiction to satisfy the Colorado requirement. DPA elements need to be tailored to risk to appropriately balance consumer protection against inhibiting business activities that, if done improperly, could harm consumers. CCIA suggests removing the requirement in draft Rule 9.06(F)(6) to require third-party software provider reports.

IX. CLARITY

A. Scope of Rights Broadcasting Obligations

The draft Rules introduce new rights broadcasting obligations that require Controllers to notify all processors that process consumers' personal data of a consumer's access, deletion, correction, and opt-out requests, including how the Controller responded to the requests. CCIA suggests the Department remove these impractical obligations for businesses and align with the broader landscape of emerging US state comprehensive privacy laws.

CONCLUSION

CCIA and its members thank the Colorado Department of Law for the opportunity to provide suggestions on how to balance the Rules in ways that protect consumer data, are feasible to implement, and retain flexibility for customization and innovation. The suggested alternative language discussed herein, which is also provided in **Attachment A** in redline form for ease of review, is offered as a means for achieving the best result for consumers, regulators, and the online ecosystem.

Respectfully submitted,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue, NW, Suite 300C
Washington, D.C. 20001
amaranon@ccianet.org

November 7, 2022

Computer & Communications Industry Association
Tech Advocacy Since 1972

ATTACHMENT A

Suggested Amendments to Proposed Rules

Rule 2.01 "Biometric Data": as referred to in C.R.S. § 6-1-1303(24)(b) means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas scan, iris scan, or other unique biological patterns or characteristics, that is used to identify a specific individual. ~~Biometric Identifiers that are used or intended to be used, singly or in combination with each other or with other Personal Data, for identification purposes. Unless such data is used for identification purposes,~~ "Biometric Data" does not include (a) a digital or physical photograph, (b) an audio or voice recording, or (c) any data generated from a digital or physical photograph or an audio or video recording. This definition does not include information collected, used, or stored for health care treatment, payment, or operations under HIPAA.

Rule 2.01 "Biometric Identifiers": ~~means data generated by the technological processing, measurement, or analysis of an individual's biological, physical, or behavioral characteristics, including but not limited to a fingerprint, a voiceprint, eye retinas, irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.~~

Rule 3.02(A)(5): Readable on all devices through which Consumers interact with the Controller, including on smaller screens and through mobile applications, if applicable. This excludes any device in which Consumers are not expected to interact by reading, including any device that does not have a surface capable of displaying text sufficient to capture the required disclosures to Consumers.

Rule 4.04(A): A Controller shall comply with an access request by providing the Consumer all the specific pieces of Personal Data it has collected and maintains about the Consumer~~, including without limitation, any Personal Data that the Controller's Processors obtained in providing services to the Controller~~."

Rule 4.04(B): Personal Data provided in response to an access request ~~must~~ should, to the extent feasible, be:

Rule 4.05(A): A Controller shall comply with a Consumer's correction request by correcting the Consumer's Personal Data ~~across all data flows and repositories and implementing measures to ensure that the Personal Data remains corrected~~. The Controller shall also instruct all Processors that maintain the Personal Data at issue to make the necessary corrections in their respective systems and to ensure that the Personal Data remains corrected."

Rule 4.06(D): If a Consumer submits a deletion request with respect to Personal Data that falls within an exception under C.R.S. § 6-1-1304, the Controller shall delete the Consumer's

Personal Data that is not subject to the exception; ~~provide the Consumer with a list of Personal Data that was not deleted along with the applicable exception;~~ and not use the Consumer's Personal Data retained for any other purpose than provided for by the applicable exception.

Rule 5.04(B): Notwithstanding 4 CCR 904-3, Rule 5.04(A), a Consumer's decision to adopt a tool that does not come pre-installed with a device, such as a browser or operation system, but is marketed ~~prominently as a privacy-protective tool or~~ specifically as a tool designed to exercise a user's rights to opt out of the Processing of Personal Data shall be considered the Consumer's affirmative, freely given, and unambiguous choice to use a Universal Opt-Out Mechanism.

Rule 5.08(A)(1): A Controller that receives an opt-out request through a Universal Opt-Out Mechanism shall treat such as a valid request to opt out of the Processing of Personal Data for purposes of Targeted Advertising, Sale of Personal Data, or both, as indicated by the mechanism, for the associated browser or device, and, if known, for the Consumer at the account level or Controller level.

Rule 6.03(A)(5): If a Controller will delete Sensitive Data Inferences within twelve (12) hours pursuant to 4 CCR 904-3, Rule 6.10, a description of the Sensitive Data Inferences ~~subject to this provision~~ that a Controller will delete within 12 hours and the retention and deletion timeline for such Sensitive Data Inferences.

Rule 6.10(B)(2): "The ~~Personal Data and any~~ Sensitive Data and/or Sensitive Data Inferences are permanently deleted within twenty-four (24) ~~twelve (12)~~ hours of collection or of the completion of the Processing activity, whichever comes first;"

Rule 6.10(B)(3): "The ~~Personal Data and any~~ Sensitive Data and/or Sensitive Data Inferences are not transferred, sold, or shared with any Processors, Affiliates, or Third-Parties; and"

Rule 6.10(B)(4): "The ~~Personal Data and any~~ Sensitive Data and/or Sensitive Data Inferences are not Processed for any purpose other than the express purpose disclosed to the Consumer."

Rule 7.08(A): A Controller that has obtained Consent from a Consumer must refresh Consent in compliance with all requirements of this Part 7 ~~at regular intervals~~ based on the context and scope of the original Consent, sensitivity of the Personal Data collected, and reasonable expectations of the Consumer.

Rule 7.09(B)(4): ~~If a Processing purpose materially evolves such that the new purpose becomes a secondary use pursuant to C.R.S. § 6-1-1308(4), the Consumer's original Consent is no longer valid, and the Controller must obtain new Consent pursuant to Part 7 of these Rules.~~

Rule 7.09(B)(9)(a): ~~Example: If it takes two clicks for a Consumer to Consent through a website, it should take no more than two actions for a Consumer using a digital accessibility tool to complete the same Consent process.~~

Rule 9.02(D): The Automated Processing used in Profiling includes Solely Automated Processing~~,~~ and Human Reviewed Automated Processing~~, and Human Involved Automated Processing~~, as defined at 4 CCR 904-3, Rule 2.02.

Rule 9.03(A)(5): ~~If the Profiling is used to serve ads related to housing, employment, or financial or lending services;~~

Rule 9.03(B): Notwithstanding the requirements in 4 CCR 904-3, Rule 9.03(A), nothing in 4 CCR 904-3, Rule 9.03 shall be construed as requiring the Controller to provide information to a Consumer in a manner that would disclose the Controller's trade secrets~~.~~ or proprietary information.

Rule 9.06(A): Controllers must conduct and document a data protection assessment compliant with C.R.S. § 6- 1-1309 and 4 CCR 904-3. Rules 8.01-8.05 before Processing Personal Data for Profiling if the Profiling is like to result in a risk of ~~presents a reasonably foreseeable risk of~~:

Rule 9.06(B): Profiling under C.R.S. § 6-1-1309(2)(a) and covered by required data protection assessment includes Profiling using Solely Automated Processing~~,~~ and Human Reviewed Automated Processing~~, and Human Involved Automated Processing.~~

Rule 9.06(F)(6): If the Profiling is conducted by Third Party software purchased by the Controller, the name of the software and sufficient information to inform the evaluation of accuracy where relevant to the risks described in CPA Section 6-1-1309(2)(a)(I-IV) (for example, copies of any internal or external evaluations of the accuracy and reliability of the software;