Computer & Communications Industry Association
Tech Advocacy Since 1972

January 18, 2023

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

Re: Revised Proposed Draft Regulations

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 revised Draft Rulemaking (the "draft Rules") governing the implementation of the Colorado Privacy Act ("CPA").

DISCUSSION

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. The revised rules greatly improve upon the initial draft and we appreciate the noteworthy changes that directly respond to previously raised issues. These comments build upon the Association's past pre-rulemaking input and focus on the provisions that still warrant further revision.

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

I. DEFINITIONS

A. Rule 2.02 – "Automated Processing"

The definition of "Human Involved Automated Processing" should be deleted and if needed, modify "Solely Automated Processing" to note that it includes human review with no ability to change the outcome. Properly distinguishing between "Human Involved Automated Processing" and "Human Reviewed Automated Processing" is operationally challenging – it is unclear how one can prove the level of consideration a human actually gave an output in order to

[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.

distinguish between the two. The "Human Involved" term is unnecessary because if the human did not have a meaningful opportunity to consider, whether due to policies or other restrictions, then it would simply be "Solely Automated Processing."

B. Rule 2.02 – "Biometric Data" and "Biometric Identifiers"

The draft Rules continue to 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. The draft rules still contain references to identifiers that might be "intended to be used." Biometric data should be limited to identifiers that are actually used for the identification of *specific persons* rather than identification generally. It is unclear how the concerns with intended use will not be addressed by any subsequent, actual use.

Accordingly, CCIA recommends defining "biometric data" in accordance with emerging U.S. state comprehensive privacy laws, striking the term "biometric identifiers" and 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]

As an alternative to striking, we have recommended further revisions to the "Biometric Identifiers" term in **Attachment A** to provide needed clarification that the data is limited to identifiers used to uniquely identify an individual.

C. Rule 2.02 – "Bona Fide Loyalty Program"

The final Rules should not seek to create more granular subdivisions for this definition. Beyond creating create confusion for consumers and organizations, it invites conflict with the statutory intent and language that permits flexibility with such programs. CCIA recommends the Department avoid this suggestion for an overly-prescriptive definition.

D. Rule 2.02 – "Employment" Terms

The final Rules should define the term "employment opportunities" to clarify that job applicants, employees, and independent contractors are exempt from the requirements relating to decision-making. The term "acting in a commercial or employment context" should be defined to

[2] Connecticut Data Privacy Act, P.A. 22-15 Section 1(3); Virginia Consumer Data Protection Act, S.B. 1392 Section 59.1-571.

include job applicants, employees, and independent contractors. Lastly, the definitions of "employment records," "employee," and "employer" should include job applicants, independent contractors, and related data.

The Association suggests the Department clarify that the requirements relating to "profiling" – including opt-out rights – do not apply to employees, job applicants, and independent contractors.

E. Rule 2.02 – "Sensitive Data Interferences"

Rather than needlessly creating a new category of data for the purpose of defining revealing, the final Rules should instead simply further clarify the meaning of "revealing." This definition should be removed.

II. CONSUMER DISCLOSURES

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

The draft Rules still do not provide sufficient language specifying the scope of the readability requirements for devices. CCIA remains concerned that the vague language could impose these requirements on devices like video platforms that consumers typically do not interact with by reading. CCIA recommends the Department clarify this readability requirement and ensure the carveout extends to headless devices and other similar devices.

III. CONSUMER PERSONAL DATA RIGHTS

A. Rule 4.03 – Right to Opt-Out

The CPA expressly removed the right to opt-out of profiling from the general rule of providing the opt-out.[3] The draft Rules, however, still eliminate this 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." The profiling opt-out under the CPA is limited to decisions that produce legal or similarly significant effects. Due to its highly contextual nature, profiling opt-outs tend to be located in the specific user experience and not generally in the privacy notice – this obfuscation may also confuse consumers on what decisions they are actually opting-out to. CCIA urges the final Rules to restore this distinction to reflect the

[3] Colorado Privacy Act, § 6-1-1306, (1)(a)(III).

statute's intent.

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."

The reference to the "app store" in draft Rule 4.03(B)(3) should be removed 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 downloads it.

Lastly, Controllers should have at least 45 days to comply with an opt-out request, similar to what is required under the VDCPA. At a minimum, Rule 4.03(A)(1) should be revised to 15 business days.

B. Rule 4.04 – Right of Access

The draft Rules continue to impose heavy compliance requirements on businesses regarding the right to access. The proposed language specifies that Controllers are to provide a consumer "without limitation" any personal data they obtained and "must include explanations that would allow the average consumer to make an informed decision" on whether to exercise their rights. These requirements create unnecessary friction for businesses and consumers, resulting in potentially longer response times to consumers as organizations rely on automated processes to respond to access requests. To ensure that businesses have the necessary flexibility to operationalize these requirements, CCIA proposes eliminating this requirement or limiting it to where the produced data is not reasonably self-explanatory.

The Association is still concerned that the trade secrets language in Rule 4.04(D) does not extend to access rights. While we recognize that this provision aims to address a tension in the statute between portability and access rights, as drafted, the provision will have the unfortunate effect of compromising industry trade secrets altogether – something the statute explicitly seeks to avoid. CCIA recommends the Department clarify that exemptions apply

broadly to both access and portability requests – absent this clarification, we recommend striking this language.

The new language in Rule 4.04(A)(1) is overly broad and vague and confusingly appears to pull into scope much more than just actual personal data. Data is consistently used to build products and services, develop analysis, and more. For example, a powerpoint presentation, spreadsheets, or other internal work product expressly using the personal data could arguably be derivates (especially where the term is undefined, like here). Further, it is not clear what is meant by inferences – if an individual conducts an analysis on a consumer population to determine that 20% of their consumers are named John, does that individual have to provide them all with this information? Providing content beyond discrete personal data seems sprawling in scope and could raise significant confidentiality and intellectual property concerns. This provision should be deleted, otherwise, products and services may not be made available to Colorado citizens if it could result in the mandatory disclosure of proprietary information. This same issue appears in the new edits to Rule 4.07.

C. Rule 4.07(B)(1) – Right to Data Portability

For similar reasons as those mentioned in Rule 4.04(A)(1), the final Rules should remove references to inferences and derived data.

D. Rule 4.09 – Responding to Consumer Requests

Despite the revisions to the Controller obligations, there continue to be concerned with this provision. Specifically, it is unclear how Controllers are to respond to a consumer request when the processor does not provide the "technical and organizational" measures contemplated in this provision. To address these implementation concerns, CCIA suggests striking this provision. For similar reasons as in 4.04(A)(1), the rules should remove references to inferences and derived data.

E. Specific Questions – Consumer Personal Data Rights

An I.P. address is a commonly used, practical geolocation method, especially in situations where it would be impractical for the consumer to affirmatively specify their location through other means. The Department should allow such methods for authentication and a business should retain the flexibility to choose a method that works best for the applicable context. For example, a real estate business with a dedicated Colorado website may choose to geolocate consumers visiting that site as located in Colorado.

IV. UOOMs

A. Rule 5.04(B) – Default Settings

The revised draft Rules still do not adequately address the concerns over default settings. As written, the provision would still contradict the statute's explicit direction that the opt-out mechanism clearly represents the consumer's "affirmative, freely given, and unambiguous choice to opt-out." Consumers might adopt a particular browser for a variety of reasons, and there is no way to verify whether the choice of browser was due to the marketed opt-out settings or an entirely unrelated reason. The proposed language would mean that the consent to the UOOM is bundled with all of the other privacy-enhancing features of the device, leading to a significant number of erroneous opt-out signals.

CCIA recommends the Department remove this provision altogether as it directly contradicts the statute with respect to default settings.

B. Rule 5.06 – Technical Specification

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 app. Otherwise, permitting alternative formats creates greater friction for companies to recognize users opt-out choices and creates further consent fatigue for customers.

The language in draft Rule 5.06(B)(2) allowing opt-outs to be limited to one or more Controllers creates a risk of abuse by UOOM developers, who could unfairly disadvantage specific Controllers. The Department should confirm that a UOOM provider should not preselect a list of Controllers.

CCIA recommends the Department provide a security standard for UOOMs and a carveout 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.

C. Rule 5.07 – System for Recognizing UOOMs

The six months grace period is welcomed, given the complexity of implementing multiple UOOMs across various web surfaces simultaneously. But the Department can still help

organizations by providing further guidance on the cadence of new designations and the total number of designations. Moreover, for any UOOMs that Controllers are required to honor, it must be free for the Controllers.

D. Rule 5.08(A) – Obligations on Controllers

The provision still requires Controllers to apply the opt-out request at the consumer level "if known." However, some Controllers consist of multiple businesses with separate customer accounts – enabling users to set different settings for different accounts. But the current language would create confusion for customers if their targeted ads preference for one service automatically carries over to another. The suggested edits aim to address this risk.

CCIA is concerned over the technical feasibility of persistently honoring consumers opt-out requests from a UOOM absent any authentication criteria. The Department should clarify that a business should continue to honor a UOOM to the extent it can continue to recognize the authenticated consumer.

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

The Department should clarify that if the UOOM technical specifications allow it to indicate that the consumer has turned the UOOM signal off, then the Controller should be able to interpret that as an opt-in with to the extent that the consumer had previously opted-out with that same Controller with that same UOOM signal.

F. Specific Questions – Consumer Personal Data Rights

Regarding the recognition of UOOMs, it should be prescribed in this rulemaking and can be revisited in future reviews.

V. DUTY OF CONTROLLERS

A. Rule 6.03(A) – Privacy Notice Content

The last sentence in Rule 6.03(A)(1)(e)(i) does not correspond with the example, goes beyond selling or sharing, and is inconsistent with the revised rules, which eliminate the requirement to tie disclosures to each processing purpose. CCIA recommends striking this sentence to avoid this inconsistency and to conform with the revised requirement in Rule 6.10, the timing language in Rule 6.03(A)(5) should be changed from "12 hours" to "24 hours."

B. Rule 6.04 – Changes to Privacy Notice

CCIA recommends deleting the fifth example regarding the identification of "Affiliates, Processors, or Third-Parties" for it substantively deviates from what the statute requires. The statute requires that the privacy notice include only "categories" of third parties, not this additional requirement concerning identities. The example language should be modified to reflect this.

C. Rule 6.05 – Loyalty Programs

Concerns remain with the prohibitive language in Rule 6.05(A) that conflicts with Rules 6.05(B)-(D) and (F). 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.

D. Rule 6.09 – Duty of Care

The revised language refers to "administrative, technical, organizational, and physical safeguards." While many of these seem like interchangeable terms, the Final Rules should match the language in the statute – "technical and organizational measures." This would align with other state privacy laws like the California Privacy Rights Act. Additionally, the reference to ensuring the "availability" of personal data in Rule 6.09(C)(2) should be removed as it is ambiguous and does not provide any clear customer benefit.

The suggested edits to Rule 6.09(C)(4) in Attachment A seek to reduce the ambiguity around Controllers' and processors' duty of care with their data security policies.

E. Rule 6.10 – Duty Regarding Sensitive Data

The proposed requirement concerning data sharing with affiliates and processors is overly burdensome without any countervailing benefit to consumers. CCIA recommends the requirement be modified to exclude situations where the data is transferred to an affiliate or to a processor (and concerning the processor, at least where the processor is acting solely on behalf of a Controller and for no other purpose).

F. Rule 6.11 – Documentation Concerning Duties of Controllers

The draft Rules requirement 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. Rule 7.03 – Requirements for Valid Consent

Draft Rule 7.03(C)(2)(a) still 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.

CCIA recommends striking draft Rule 7.03(D)(1)(a) and (D)(2) in their entirety. The current language, by implication, requires individual consent for every purpose, even if those purposes are related and compatible. The revision doubles down on this departure by adding subclause (D)(1)(a), which provides that Controllers may present consent to processing personal data for multiple related or similar processing purposes, *so long as there is an option for more granular consent*. This is unreasonable and overly burdensome given the complex nature of providing services using personal data, and it risks creating consent fatigue.

Draft Rule 7.03 (E) remains overly broad, imposing a significant burden on companies and confusion for consumers to the extent it would require detailed disclosures whenever a consumer chooses to opt-in. Consumers often toggle back and forth between opt-in and opt-outs settings on a control page, so additional disclosures that must appear whenever the consumer opts-in creates unnecessary friction. Consumers also 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 recommends the Department strike this requirement in its entirety or limit it to certain high-risk situations. However, if this provision remains, at a minimum, the Department should include a carve-out for where a consumer opts-in after opting-out, such as relating to targeted advertising or profiling. This would require a similar edit to Rule 7.05 concerning consent after opt-out. This burden is further compounded by revised Rule 7.04(C) which does not permit consent disclosures to point back to the privacy notice.

B. Rule 7.04 – Requests for Consent

Draft Rules 7.03 and 7.04, when read together, risk imposing substantial friction and clutter for consumers looking to manage their data preference settings. Companies should retain discretion in designing a landing page where consumers may control the settings. To the extent a company must include the full range of disclosures for consent under Rule 7.03, the company should be able to rely on the disclosure in the privacy notice. Since the requirements under Rule 7.03 are so varied, the company cannot point to a single section of the privacy notice.

C. Rule 7.06(A) – Consent for Children

The final 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. CCIA strongly advises the Department to remove 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.

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.

D. Rule 7.07 – Refusing or Withdrawing Consent

Draft Rule 7.07(E) still imposes burdensome requirements for organizations. The language requires a business to surface deletion instructions each time a consumer modified a processing preference – such as opting in or out of targeted advertisements. To avoid this unnecessary burden on business and possible disruption to consumer experience, the Department should confirm that it is sufficient for a business to disclose in its privacy notice how a consumer can exercise their deletion right.

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

The language in revised Rule 7.09(A)(4) is still 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.

VII. DATA PROTECTION ASSESSMENTS

A. Rule 8.02 – Scope

To avoid unnecessary confusion, CCIA recommends the Department update the reference to "heightened risk of harm" in Rule. 8.02 to match the CPA definition in Section 6-1-1309.

B. Rule 8.05 – Timing

CCIA recommends the Department clarify that the data protection impact assessment requirement applies only to data acquired on or after the effective date. This would align with the statutory text in Section 6-1-1309(1). Further, under Rule 9.06(A), a DPA for profiling is only required under certain circumstances. Draft Rule 8.05(C) needs to be revised to ensure that annual review and update applies only when a DPA is required under Rule 9.06.

VIII. PROFILING

A. Rule 9.02(B) – Scope

While the term "automated processing" remains undefined, it would be helpful to clarify that the opt-out right excludes automated processing that is "accessory to the evaluation, analysis, or prediction, such as the use of calculators or spreadsheets."

B. Rule 9.03 – Profiling Opt-Out Transparency

Despite the revisions to provisions concerning profiling, concerns remain over the scope of protections afforded in Rule 9.03(B). The Department should extend these protections beyond only trade secrets to include "proprietary information" and afford the same to DPAs as described in Rule 9.06(F).

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

The final Rules should not impose any further burdens on human involved automated processing. If the idea is to ensure fairness, the final Rule should not extend the scope of this provision to decisions where humans assessed the information and made a decision.

D. Rule 9.06 – Data Protection Assessments for Profiling

Concerns remain with the obligations provided in Rule 9.06(A). To maintain parity with other privacy regimes, a DPA should only be required where a risk is *likely to result* – as under the GDPR – rather than "reasonably foreseeable." In addition, for Rule 9.06(A)(3), CCIA proposes striking "or other intrusion." It remains unclear what "a physical or other intrusion upon the solitude or seclusion, or private affairs or concerns" constitutes as it applies to digital privacy. This concept is well-established in tort law, and commonly applies to physical spaces. It does not easily equate to virtual spaces and including this provision unreasonably expands the possible scope of the law. The Department can also alleviate some of the burdens with these assessments by adding "where relevant to the risks" to the whole profiling DPA scheme, meaning a company only has to provide information to the extent that it is related to the specific risks that trigger the DPA.

The language in Rule 9.06(B) should be modified further to ensure the regulation of profiling excludes human-involved reviews for the aforementioned reasons.

The DPA requirement concerning the type and degree of potential harm to consumers should only apply to truly high-risk scenarios where heightened oversight is needed. The reference to a "small harm to a large number of consumers" in Rule 9.06(E) should be removed.

The language in Rule 9.06(F) still warrants further revision. CCIA suggests removing the requirement for DPA elements to require third-party software provider reports. DPA elements should be tailored to risk in order to balance consumer protection against slowing down business activities, which can also pose harm to consumers.

Lastly, CCIA suggests adding "where relevant to the risks" to the profiling DPA elements in Rule 9.06(G). This will require a company to provide information only to the extent that it is related to the specific risks that trigger the DPA.

IX. ENFORCEMENT

A. Rule 10.02(A) – Enforcement Considerations

Given that the implementing regulations will likely not be finalized until close to or potentially after the CPA effective date, CCIA suggests the Department consider the amount of time between the effective date of the regulations and the possible or alleged violations. This

additional consideration would provide further relevant facts for the Department's assessment and align with other state privacy laws like Section 7301(b) of the CPRA.

CONCLUSION

CCIA and its members thank the Colorado Department of Law for the several opportunities to provide suggestions on how to balance the final regulations 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

January 18, 2023

ATTACHMENT A

Suggested Amendments to Revised Draft 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 that ~~can be~~ are Processed for the purpose of uniquely identifying an individual, 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 4.03(B)(3): positioned in an obvious location of a website or application, such as the header or footer of a Controller's internet homepage~~, or an application's app store page or download page~~;

Rule 6.03(A)(1)(e)(i): For example, categories of Third Parties described in a sufficiently granular level of detail include, but are not limited to: "analytics companies," "data brokers," "third-party advertisers," "payment processors," "lenders," "other merchants," and "government agencies." ~~For each processing purpose, whether the Personal Data collected is Sold or processed for Targeted Advertising.~~

Rule 6.04(A)(1): Substantive or material changes may include, but are not limited to, changes to: (1) categories of Personal Data Processed; (2) Processing purposes; (3) a Controller's identity; (4) the act of sharing of Personal Data with Third-Parties; (5) the ~~identity~~ categories of Affiliates, Processors, or Third-Parties Personal Data is shared with; or (6) methods by which Consumers can exercise their Data Rights request.

Rule 6.05(A): ~~While a Controller may not increase the cost of or decrease the availability of a product or service based solely on a Consumer's exercise of a Data Right, a~~ A Controller is not prohibited from offering Bona Fide Loyalty Program Benefits to a Consumer based on the

Consumer's voluntary participation in that Bona Fide Loyalty Program. However, the Bona Fide Loyalty Program Benefit must be reasonably related to the value provided to the Controller by the Consumer's Personal Data.

Rule 6.09(C)(4): Ensure that Controllers and Processors comply with their respective ~~compliance with~~ data security policies ~~by the Controller and Processors~~.

Rule 7.04(C): Any interface used by a Controller to request a Consumer's consent must contain the disclosures required by 4 CCR 904-3, Rule 7.03(E)(1). The request interface itself must contain the disclosures required by Rule 7.03(E)(1)(a)-(d) ~~and~~ or the Controller may provide the Consumer with a link to a webpage containing the Consent disclosures required by 4 CCR 904-3, Rule 7.03(e)-(g)~~, provided the request clearly states the title and heading of the webpage section containing the relevant disclosures~~. If technically feasible, the request method must also link the Consumer directly to the relevant section of the disclosure.

Rule 9.06(A)(3): A physical ~~or other intrusion~~ upon the solitude or seclusion, or private affairs or concerns, of Consumers if the intrusion would be offensive to a reasonable person; or

Rule 9.06(A)(3): If the Profiling is conducted by Third Party software purchased by the Controller, name of the software and sufficient information to inform 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).

Rule 9.06(G): If a Controller is Processing Personal Data for Profiling under C.R.S. § 6-1-1309(2)(a), a data protection assessment of that Processing activity where relevant to the risks must include the elements listed at 4 CCR 904-3, Rule 8.04 as well as each of the following: