Computer & Communications Industry Association
Tech Advocacy Since 1972

July 29, 2022

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

Attorney General Weiser:

The Computer & Communications Industry Association ("CCIA")[1] is pleased to provide input on the preliminary rulemaking under the Colorado Privacy Act, or "CPA".

CCIA supports the State of Colorado in its efforts, which are among the first in the nation, to adopt and implement a comprehensive privacy law. Though certainly your Office is authorized to implement the CPA in your best judgment, we request that Colorado remain mindful that until a federal privacy law of common application is enacted, America's industries must comply with a growing number of state laws that often adopt disparate standards for addressing the same issues. Regulations that support state-to-state consistency is a valuable goal for both industry and consumers.

The forthcoming rules should protect consumers while providing a clear roadmap for innovative businesses to comply. In addition, they should strive to be technology-neutral to avoid creating barriers to innovation and prevent skewing the competitive playing field. Perhaps most importantly, the rules should be normative rather than prescriptive – rules should set standards of conduct that must be followed rather than endorse or condemn any specific feature or design choice. Confining the rules to today's practices necessarily invites circumvention through invention and will quickly render the rules obsolete.

The following tenets of privacy policy are crucial for achieving these goals:

[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.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

I. UNIVERSAL OPT-OUT

The rules should provide principles for a universal opt-out mechanism (UOOM), rather than prescriptive norms. Above all, the UOOM rules should not impede innovation, endorse particular features or technologies, or create a regime that results in consumer "consent fatigue". Standardization, predictability, and adequate notice are critical to enabling consumer preferences in a timely manner while avoiding unreasonable burdens on the ability to serve customers.

1. The Rules Should Adopt a UOOM that Is Universal, Unburdensome, and the Product of Collaboration.

The universal signal should not be left to any single organization to create. It should be created with the required input from industry so that no single entity exerts outsized influence over the signal's standards. Successful solutions are driven by, or developed in collaboration with, industry groups, which are a key source of subject matter expertise. This expertise concerns both technical feasibility as well as the practical requirements of the various types of marketplace participants.

Requirements to honor UOOMs should not exceed the capabilities of eligible UOOMs that are available in the marketplace. For example, if only browser extensions can serve as UOOMs, the requirement to honor UOOM signals should only extend to browsers. Additional details about the categories of tools that would be eligible to serve as UOOMs will allow businesses to understand the various locations/surfaces where preferences should be recognized. As new locations/surfaces become available, UOOM regulations will need to evolve and adapt to accommodate those contexts.

The regulations should limit the number of signals to a minimum to prevent conflict among signals if each one had different standards and if customers sent conflicting signals. They should also allow customers to opt in/reverse any opt out selection. Absent these requirements, multiple entities may create competing signals with different standards. As a result, businesses and customers alike would suffer from significant compliance costs and confusion about how to exercise their opt-out rights and thus experience consent fatigue.

2. The Rules Should Set Forth Clear Technical Standards for UOOMs.

The regulations should identify specific standards and specifications to govern the UOOM. More specifically, the rules should (1) restrict the range of signal types for which a business must build infrastructure to receive, and (2) restrict the number of applicable UOOMs that a

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

customer must activate in order to prevent consent fatigue.

Regulations that include clear specifications will help ensure that UOOMs are usable because they will facilitate standardization, stability, and predictability. They will also help businesses ensure and maintain compatibility, because integration with external signaling mechanisms is often a lengthy, complex, and resource-intensive effort for signal recipients. Updates to the specifications and standards should be made periodically, however changes should not be permitted without notice, opportunity to comment, and regulatory approval. UOOM providers should also be prohibited from introducing other changes to the UOOMs without providing appropriate notice and following a specified process, as these modifications would impact the recipients' ability to receive and honor the legally required signals.

The specifications should include the following requirements:

- UOOMs must not introduce additional preferences or hurdles that would gate access to the legally required signals. Honoring any additional signals not mandated by law should be optional and not a compliance obligation.
- UOOM technical standards should enable businesses to immediately recognize whether a given UOOM is a legitimate UOOM 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.
- The specifications and standards should include security measures that would prevent a bad actor from sending false opt-out signals or using the signals to gain unauthorized access to a receiving company's systems or consumer data.

Colorado also should adopt clear rules regarding the accountability and oversight of UOOM providers. There should be an exemption from liability for businesses if a UOOM provider discontinues or fails to maintain their UOOM in accordance with the applicable requirements. Similarly, the regulations should be designed to prevent a situation where a widely adopted privacy preference mechanism is called into question by the regulator ***after*** the rules are adopted, as we have seen with the recent Transparency & Consent Framework (TCF) decision out of the EU.[2]

CCIA notes that the CPA currently requires the regulator to develop specifications for sale of

[2] Belgian Data Protection Authority, *Decision on the Merits 21/2022 of 2 February 2022, Complaint Relating to Transparency & Consent Framework (IAB Europe)*, DOS-2019-01377, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

data and targeted advertising opt-outs, but not for the profiling-related opt-out. We recommend that the specifications address ***all*** opt-out preferences that consumers may express via UOOM under the CPA.

Finally, Colorado should provide adequate notice of any UOOM specifications and standards with a reasonable timeframe for compliance. It will take time for the UOOM providers to develop the signals and for businesses to be able to build infrastructure to recognize, receive, and honor a new or modified signal.

3. The Rules Should Ensure UOOM Interoperability.

Ideally, a UOOM would be interoperable with any number of technologies *(i.e.*, browsers, apps, streaming TV, headless devices, etc.). However, we are not aware of any such existing UOOM to date, and designing one that will work across the different types of technologies is likely a nontrivial matter. For instance, a UOOM that is compatible for a browser may not be practical for a headless device or an offline setting.

Regulations should consequently acknowledge that the technical ability to receive and recognize certain types of signals may be limited to the particular service or device receiving the signal — a signal expressed by a browser extension when the user is logged out of a receiving service may only feasibly be recognized for that particular service, and not across the entirety of the business that operates the service.

Finally, regulations should be flexible enough to allow businesses to continuously innovate and develop new, technology-enabled solutions for customers.

4. Colorado Should Aim for Regulatory Consistency Regarding UOOMs.

We recommend that Colorado regulators remain aware of other states' privacy preference requirements when designing UOOMs, in order to provide a consistent consumer experience wherever possible and to avoid imposing incompatible and overly onerous demands on the industry. This standard should apply both to the choice of permissible UOOMs as well as the types of legally mandated consumer preferences transmitted through them.

In particular, the regulations should confirm whether the Global Privacy Control (GPC) is an acceptable UOOM for purposes of the CPA. The Attorney General of the State of California has previously indicated, via tweet, that the GPC may be an acceptable opt-out method for purposes of the California Consumer Privacy Act ("CCPA"), which is some indication of regulatory sentiment in that state. However, we are not aware of any formal rulemaking by the

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

California regulator regarding the suitability of the GPC under either the CCPA or the California Privacy Rights Act. In general, to the extent that any specific UOOM providers or UOOMs are endorsed or approved by regulators, such endorsement or approval should be promulgated as part of a formal administrative process and not through informal channels.

II. CONSENT

1. The Rules Should Adopt a Flexible, Broad Standard "Clear, Affirmative Act" in Order Not to Stymie Innovation.

The regulations should take a flexible approach for what qualifies as a "clear, affirmative act" manifesting consent. A flexible approach will facilitate customer experiences across a range of devices and services. Consent must not, however, be construed from silence or inaction.

Most importantly, the regulations should not prescribe required forms of consent. This is particularly important where certain forms of consent might not be compatible across technologies. For example, some devices that are voice activated do not have a physical interface and, therefore, consumers should have the option to provide verbal consent. This approach avoids burdening the consumers with complicated multi-step consent processes.

The regulations should also recognize that a consumer consents through an affirmative act when he or she knowingly and intentionally discloses 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 the collection and processing of that demographic data.

2. The Standard for "Specific", "Freely Given", and "Unambiguous" Consent Should Be Similarly Flexible.

The regulations should define "specific" consent broadly enough to cover a range of data types and data uses. Regulations should not prohibit a company from offering customers the option to provide a one-stop shop for providing consent for how their data is used across experiences. For example, when setting up consent permissions for a child, the rules should not prevent a parent from having the option to provide a single consent for different types of personal data or for processing data for different experiences such as music and video.

Regulations should be designed to help businesses understand how to manage inconsistent consumer preferences. For example, the regulations should clarify the expected opt-out behavior if a consumer has expressed conflicting preferences on a single browser or device via

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

two different UOOMs, or via a UOOM and a consent mechanism on the controller's site. This could also apply when those preferences may originate from two different sets of legal requirements, like Colorado's and another state's or country's consent standards.

The regulations should also prohibit the use of ***pre-selected*** opt-out options, which would direct consumer decision-making toward one or more pre-set outcomes. 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.

In scenarios where a UOOM provides more choices than are required by law, businesses should have the option to determine how to manage those choices, as opposed to having to receive and recognize all of them. Receiving and recognizing ***all*** choices is both technologically and practically infeasible – businesses should not be required to confer some benefit to a consumer just because the option to request such a benefit is included in the UOOM. In addition, UOOMs should not be permitted to introduce additional hurdles or preferences that would gate access to legally required signals.

The standard for "freely given" consent should require that a consumer is provided with genuine choice and control over their data. Consumers should not be forced to provide consent. Requiring consumers to provide consent as a condition to use a service makes refusal impossible. Further, "unambiguous" consent should require an affirmative action demonstrating explicit agreement to terms.

3. "Informed Consent" Should Be Deemed Valid If Properly Obtained at the Outset of the Relationship

Regulations should not define "informed consent" in a way that limits a company to 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.

Controllers should be permitted, but not required, to authenticate consumers when honoring choices transmitted through eligible UOOMs. Numerous opt-out solutions presently in use (*e.g.*, Digital Advertising Alliance's AdChoices, the Network Advertising Initiative's interest-based ads opt-out, and various providers' own solutions) do not require authentication, and neither does the GPC. Omitting authentication in order to support opt-outs poses low risk to

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

consumers, especially if standards are in place to determine what kinds of UOOMs qualify to transmit those signals.

To the extent the rules require authentication, controllers should have flexibility to use "reasonable mechanisms" (or similar) to authenticate a consumer's residence, and those requirements should be technology-neutral.

4. The Rules Can Borrow from Existing, Proven Consent Mechanisms.

With regard to authenticating consent, Colorado can look to mechanisms already proven to work in other contexts. For example, to authenticate that the user setting up child permissions is an adult, the rules should state that reasonable consent mechanisms include phone number or credit card code (CVV) authentication.

In the EU, the TCF has been established as the mechanism for complying with the General Data Protection Regulation with respect to consumer notice. TCF gives businesses a common language for informing consumers about what data is being collected and how it might be used by third parties. The market responded by developing Consent Management Platforms, which are applications built on TCF standards that collect and signal user preferences. In Colorado, adoption of a similar framework would routinize and simplify consent for consumers and streamline compliance.

III. DARK PATTERNS

1. The Rules Governing Dark Patterns Should Apply to Conduct Rising to the Level of Consumer Fraud.

The CPA's definition of "dark patterns" is overinclusive. Every user interface requires a designer to consider an infinite range of choices that will impact user behavior. There should be a clear threshold of conduct that a business must meet before any set of design choices can be deemed a "dark pattern. "

The rules therefore should focus the definition of "dark patterns" on design practices that amount to consumer fraud, or instances that are most harmful to consumers. The "consumer fraud" approach is a well-developed and highly effective standard understood by regulators, businesses, and consumers alike. This approach would target design practices that deceive consumers into taking a desired action, such as by misleading customers about the consequences of providing or refusing consent, intentional designs that make it difficult to unsubscribe or cancel from a service, or a website that sneaks items into a consumer's online

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

shopping cart.

Conversely, Colorado should avoid regulations that would interfere with design choices that seek to promote or facilitate benefits to customers while navigating a product or service experience.

2. The Rules Should Not Prohibit Specific, Extant Design Practices, Because They Would Quickly Be Superseded Through Innovation.

Because dark patterns are context specific, the regulations should not prescribe specific types of practices. Similar to security vulnerabilities, regulators and businesses cannot identify all ways that a design may operate as a dark pattern. Instead, the regulations should rely on guiding principles that aim to avoid outcomes where consumers are misled or deceived.

The Department should rely on guiding principles, rather than prescribe specific practices, in order to promote innovation and to be compatible with emergent technologies. For instance, a rule that mandates a check box or minimum number of clicks would not be compatible for technologies that do not have a physical interface such as a voice-assistance device.

IV. DATA PROTECTION ASSESSMENTS (DPAs)

1. DPAs Should Be Limited to Circumstances Involving a Heightened Risk of Concrete, Material Harm to Consumers.

DPA requirements should be limited to processing that has a legal or similarly significant effect on an individual — where it materially affects a decision that will impact housing, education, employment and other areas protected from discrimination under the law.

From a security risk perspective, this provision should be limited to processing of data that, if compromised, is likely to result in real, concrete harms to individuals. Examples may include identify theft/fraud, extortion, or physical injury from disclosure of intimate or other objectively sensitive personal details such as gender identity.

Processing of personal information in any context for fraud prevention, anti-money laundering processes, screening, or to otherwise comply with legal obligations should be exempted from the scope of this definition/regulation. These activities protect consumers' privacy and security and such activities are treated as confidential to prevent bad actors from gaining insight into our internal systems.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

2. DPA Standards Should Be Flexible to Account for Processes That a Business Already Has in Place.

As CCIA already has stated in multiple contexts, Colorado's rules implementing the DPA provisions of the CPA should be normative, not prescriptive. Businesses should be able to structure the DPAs in a manner that reflects their internal functional organization. Regulations should avoid an artificial grouping of requirements that would be operationally burdensome and would also be a less realistic assessment of the relevant processing activities.

3. DPAs That Businesses Conduct for Other States Should Be Presumptively Compliant in Colorado.

To promote interoperability and harmonization, Colorado should align with DPA requirements under other privacy laws, including those that will come into effect in 2023, such as the Virginia Consumer Data Protection Act (VCDPA). In fact, the DPA provisions in the CPA closely resemble the requirements in the VCDPA,[3] and so the Department should not issue regulations that would deviate from how companies comply with DPA rules under the VCDPA.

The regulations should recognize that risk assessments are an increasingly common requirement under U.S. and international privacy and data protection laws. To promote interoperability and minimize burdens to covered businesses, the regulations should specify that the Department will accept risk assessments that were conducted pursuant to a comparable legal requirement. The rules should also include a requirement to notify consumers when high-risk activities cannot be remedied.

Adopting a consistent standard across jurisdictions would enable businesses to continue to build robust systems to protect consumer information. These systems will benefit from clear guidelines that allow businesses to innovate and develop their data protection assessments and properly assess their cybersecurity risks.

V. AUTOMATED DECISION-MAKING

Automated decision-making benefits consumers and businesses with accuracy, consistency, safer and innovative products, scalability, cost savings, and higher efficiency. The forthcoming rules regarding automated decision-making therefore should be tailored to address specific, known potential harms to consumers. Further, the rules should be targeted only to automations that result in ***final*** decisions affecting a consumer. In addition, the rules should

[3] Virginia Consumer Data Protection Act, S.B. 1392 Section 59.1-576, https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

focus on the expected results of the process rather than its nature (manual versus automated).

CCIA recommends that regulations continue to implement the high-risk approach concerning automated decisions having legal or similarly significant effects regarding the consumer's personal data.

Finally, CCIA notes that the CPA regulates this activity only as to consumers and does not cover profiling in the business-to-business context.

1. The Transparency Rule for Automated Decision-Making Should Adopt a Standard, Not a Specific Technology or a Function.

Any regulations that require disclosures about automated processing should be limited to a general explanation of technology functionality, rather than information on specific decisions made. This might include a description of 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. Companies should be able to provide this information via a publicly available disclosure on their webpage. Consumers would receive minimal or even decreased benefit from a more detailed description of complex algorithms.

In addition, the regulations should avoid disclosure obligations that conflict with the intellectual property, trade secret, and other legal rights of the business in question.

The Colorado Department of Law should provide guidance on developing concise notices that explain the relevance and purpose of the automated decision-making and the categories and use of the personal data processed. To provide transparency that meaningfully allows consumers to understand the impact of profiling, CCIA recommends that transparency notices regarding the automated processing of consumers' personal data be clear, accessible, and limited to general explanations of technology functionality. Such notices addressing how automated decisions are made may include descriptions of the types of personal data used without providing information on specific decisions made. Consumers should be able to make informed opt-out decisions by viewing companies' existing website disclosures and publicly available transparency notices.

The level of transparency should be proportionate to the level of risk associated with the automated decisions. Regulations should ensure that businesses shall only be obligated to disclose explanations for high-risk automated decisions that have legal or similarly significant effects regarding the consumer's personal data. Enforcing disclosures for low-risk automated

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

decisions would provide no benefit to consumers while simultaneously impeding business activity and unnecessarily diminishing the personalization of consumer services. All regulations, including those specifically regarding the transparency of automated processing, should not require the disclosure of trade secrets or business sensitive information. Such disclosures would have a chilling effect on customer service, innovation, and speech while providing no benefits to consumers.

2. Negative Impacts of Opt-Out Rights

To prevent negative impacts on consumer benefits, CCIA recommends that the Colorado Department of Law craft opt-out regulations to avoid interference with a business' ability to process data for purposes such as fraud prevention, anti-money laundering processes, screening, or for activities relating to security, compliance, and legal obligations.

The consumer opt-out provision may impede a core function of a business in circumstances where the high-risk automated decision-making is necessary to carry out a service. To mitigate the negative impact of the opt-out provision, businesses should be required to demonstrate that supplemental precautions are taken to protect personal data rather than provide the consumer the opt-out request. Such precautions may include rigorous testing, corroboration of results, continuous monitoring, and appeals or complaint processes. To mitigate harms to competition, CCIA recommends that regulations prevent opt-out selections for the purpose of unfairly disadvantaging other businesses.

3. Human Oversight in "Partial" Automated Decisions

In keeping with the CPA's general approach of reserving stringent regulation for high-risk actions having legal or similarly significant effects, the forthcoming rules should state that manual review of automated decision-making is limited to those circumstances. Limiting the need for manual review to the higher-risk cases prevents escalating costs and the slowing of access to services.

To determine whether an automated decision includes human oversight, the regulations should take a holistic view of the process. This approach would focus on final decisions that are not subject to human oversight, rather than intermediate uses of automated decision-making that narrows manual review to higher-risk cases. For instance, individuals receive faster access to services if businesses can quickly identify low fraud risks. This is only possible at scale using either simple algorithms – such as approving transactions with no prior fraud flags – or more complex algorithms including ones using machine learning. Then, for the smaller set of fraud risk cases, businesses can use manual review to make final decisions, such as through an

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

appeals process. In these situations, if non-final decisions – cases flagged only by algorithms for further human review – are regulated, then consumers will receive slower access to services, and will incur higher costs from increased, and unnecessary, manual review.

4. The Rules Should Not Attempt to Resolve Issues Already Addressed by Existing Laws.

The CPA should establish an additive set of consumer rights and remedies, not a duplicative one. To the extent that your Office has concerns about how automated decision-making might be misused to discriminate against a consumer or class of consumers, the CPA should not be employed as a tool for redressing such discrimination. Existing civil rights law, whether based on automated or manual processes, is the more apt and better-developed legal framework for such violations. The forthcoming CPA regulations therefore should tailor consumer protection in the content of automated decision-making to those that are not already covered by existing law.

5. The Rules Should Exempt Automated Decision-Making Related to Fraud, Security, and Criminal Activity.

To the extent covered by the definition of "profiling" ultimately adopted by the regulations, there should be appropriate carve-outs for any processing relating to fraud prevention, anti-money laundering processes, screening, or for other type of security or compliance activities. Failure to do so may enable bad actors to opt out of automated processes that detect and block their fraudulent activities, and limit companies' ability to protect customers' privacy and security.

VI. RIGHTS OF CONTROLLERS IN MANAGING PROCESSORS

The rules should clarify the role of controllers, defined in the CPA as entities that "determine the purposes for and means of processing personal data," with regard to how processors handle data. Section 6-1-1305(3) of the CPA is unclear as to controller oversight of the subcontractor process. The language could be interpreted that controllers have this unequal power over processors. Such a reading would require clearing each subcontractor arrangement with each controller.

To avoid imposing this burden on processors, the rules should simply require notice to the controller of all appointments of subcontractors that have access to the personal data of the controller's Colorado consumers. Processors should be trusted to adhere to the CPA in their own rights. Endowing controllers with the right to review and reject a processor's

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org

subcontractors would be an unnecessary additional step garnering little or no additive consumer protection.

The same clarification should apply to annual audits under Section 6-1-1305(5)(d). The rules should make clear that controllers do not have the authority to impose all costs of audits on the processor or to choose the auditor. Absent such restrictions, the costs of CPA compliance would be disproportionately thrust upon the processor. The recently enacted privacy statutes in Virginia[4] and Connecticut[5] allow processors far more autonomy in the audits process, and this same arrangement is equally appropriate for Colorado.

* * * *

Thank you for the opportunity to comment on the Colorado Department of Law's preliminary rulemaking activities under the Colorado Privacy Act. If your Office would like any further information regarding these comments and recommendations, please contact me at kboender@ccianet.org.

Sincerely,

Khara Boender
State Policy Director
Computer & Communications Industry Association

[4] Virginia Consumer Data Protection Act, S.B. 1392 Section 59.1-575(B), https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf.
[5] Connecticut Data Privacy Act, P.A. 22-15 Section 7(b), https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF.

25 Massachusetts Avenue NW, Suite 300C • Washington, DC 20001 • Ph: +1 (202) 783-0070
First Floor • Rue de la Loi 227 • B-1040 Brussels • Belgium • Ph: +32 2 661 2020
www.ccianet.org