November 7, 2022

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

RE: Future of Privacy Forum comments on Colorado Privacy Act proposed draft rules in advance of stakeholder sessions

Dear Attorney General Weiser and Members of the Colorado Department of Law,

The Future of Privacy Forum (FPF) welcomes this opportunity to provide feedback on the Colorado Privacy Act (CPA) draft rules to inform the Colorado Department of Law's public stakeholder sessions.[1] FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally. FPF seeks to support balanced, informed public policy and equip regulators with the resources and tools needed to craft effective rules.[2]

The draft rules are a testament to the Office of the Attorney General's principle-guided approach to rulemaking and we appreciate that the Department is providing numerous opportunities for members of the public and interested stakeholders to participate in the regulatory process. FPF's comments are directed towards clarifying potential areas of ambiguity to best ensure that Coloradans understand and benefit from the rights and protections established by the CPA.

Specifically, we recommend that the rules:

(1) encourage the development of Universal Opt-Out Mechanisms that facilitate compliance with Colorado's requirements for determining residency and user intent;
(2) clarify the intended scope of restrictions on "Dark Patterns" interfaces;
(3) consider the unique risks and differences in potential harms posed by information falling under the proposed "Biometric Data" and "Biometric Identifiers" definitions to ensure that the regulatory approach taken best serves the intention of the CPA; and
(4) align the protections for children's privacy and relevant definitions with the Children's Online Privacy Protection Act (COPPA).

[1] Colorado Department of Law, Colorado Privacy Act Proposed Draft Rules (Oct. 10, 2022), https://coag.gov/app/uploads/2022/10/CPA_Final-Draft-Rules-9.29.22.pdf.
[2] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.

1. Universal Opt-Out Mechanisms

As the only topic on which the CPA requires the promulgation of implementing regulations, the Department's draft rules appropriately give significant attention to resolving technical and policy questions for the exercise of consumers' rights to opt out of data sales and targeted advertising through Universal Opt-Out Mechanisms (UOOMs). In particular, FPF welcomes Rule 5.07, directing the establishment of an authoritative system identifying valid UOOMs. This system will support certainty for both consumers and regulated entities in the adoption and use of UOOMs.

In proceeding with formal rulemaking, FPF recommends that the Department consider modifications to Part 5 concerning UOOMs that will: (A) provide additional guidance for authenticating the residency of individuals using a UOOM, (B) account for potential circumstances where an otherwise valid UOOM is either transmitted or implemented by intermediaries in a deficient manner, (C) address the unique challenges posed by "do not sell" lists that operate as UOOMs, and (D) clarify the application of the rules to 'on by default' UOOMs.

A. Provide Additional Guidance on Appropriate Procedures for Authenticating the Residency of a UOOM User

The Department's draft rules recognize that in many cases certain collection and processing of information will be necessary to authenticate that the individual enabling a UOOM is a resident of Colorado.[3] However, the rules do not provide specific standards or examples of what practices would qualify as accurately authenticating Colorado residency consistent with the CPA.[4] While the Colorado Privacy Act does not necessarily require that final rules provide greater specificity on residency authentication, significant disagreement between stakeholders as to what would constitute valid authentication has emerged through public comments, suggesting that further regulatory guidance could support the effective operation of UOOMs in practice.[5]

---

[3] Rule 5.06(E)(1), Rule 5.05(B).

[4] Colorado Privacy Act [hereinafter "CPA"] § 6-1-1313(2)(f).

[5] *See* Keir Lamont & Chloe Suzman, "'The Colorado Effect?' Status Check on Colorado's Privacy Rulemaking," Future of Privacy Forum (Sept. 21, 2022), https://fpf.org/blog/the-colorado-effect-status-check-on-colorados-privacy-rulemaking/ ("Numerous commenters expressed concern that establishing strict authentication procedures could have the effect of frustrating consumer intent in exercising their privacy rights and suggested regulatory workarounds. For example, the Colorado Privacy Policy Commission suggested a standard that opt-out signal authentication must require no more than three steps to complete. Separately, several organizations including Consumer Reports and the Network Advertising Initiative (NAI) suggested that regulations could permit authenticating residency with a user's IP address. However, the State Privacy and Security Coalition (SPSC) and TechNet raised concerns about VPNs and other technologies that can make determining location by IP addresses unreliable, and further posited that the CPA may raise Constitutional concerns if enforcement of opt-out mechanisms extends beyond authenticated Colorado residents.").

In situations where a covered entity receives a valid UOOM signal (or other expression of intent to invoke applicable privacy rights) and the residency of the consumer is not already known to the covered entity, the rules should specify how covered entities can reasonably authenticate whether the UOOM is being used by a resident of Colorado. Prior commentators have suggested practices for authenticating residency based on associated information like an IP address, or asking a user to submit attesting information, such as their Zip Code. However, there are potential benefits and drawbacks to each approach. For example, commercial tools for geolocating a user based on an IP address can be useful for broad approximate inferences. However, accuracy is not guaranteed because devices and browsers are shared, used while traveling, or may use Virtual Private Networks (VPNs) or other masking technologies. Furthermore, this approach is less reliable in certain contexts, particularly for mobile devices.[6] At the same time, manually collecting additional information from users in order to authenticate residency could result in overcollection of data, unnecessary friction, and a poor user experience. FPF recommends that the Department provide illustrative examples of appropriate processes that covered entities may undertake to authenticate residency upon the receipt of a UOOM signal. Furthermore, the Department should consider supporting the development of UOOMs with features that directly convey a user's residency to recipient businesses and nonprofits.

B. Provide Greater Certainty for Covered Entities in Determining that UOOMs Reflect a Legitimate Expression of User Intent

FPF welcomes the decision for the Department to establish a public list of valid UOOMs that meet the requirements of the CPA and implementing rules. In order to provide greater certainty for the operation of UOOMs, we recommend that the Department take additional steps to ensure that stakeholders are able to determine not only that a particular UOOM specification is valid, but that UOOM signals are conveyed by intermediaries in a manner that reflects a user's "affirmative, freely given, and unambiguous choice."[7]

To illustrate this issue, consider the Global Privacy Control (a single signal specification developed to invoke opt-out rights pursuant to the California Consumer Privacy Act) that lists 7 distinct "Founding Organizations" - including web browsers and browser extensions - that can transmit the signal.[8] In the current market, the Global Privacy Control signal can also be transmitted by several apparently unaffiliated browser extensions.[9] Across these distinct signal-transmitting mechanisms, there are significant differences in relevant disclosures and functionality including consumer notices, default settings, and ability for users to exercise choice and control.[10] Furthermore, businesses receiving a Global Privacy Control signal may not have the

---

[6] *See e.g.*, Christopher Luna, "How accurate is IP geolocation?" MaxMind (July 1, 2021), https://blog.maxmind.com/2021/07/how-accurate-is-ip-geolocation/.
[7] CPA § 6-1-1313(2)(c).
[8] Global Privacy Control, "Founding Organizations" (last accessed Nov. 4, 2022), https://globalprivacycontrol.org/orgs.
[9] This includes the browser plug-ins "Crumbs," "Startpage Privacy Protection," and "GPC Enabler."
[10] *See* Keir Lamont & Jason Snyder, Future of Privacy Forum CPPA Public Comment (Aug. 23, 2022) https://fpf.org/wp-content/uploads/2022/08/FPF-CPPA-Public-Comment.pdf.

means of determining the specific source of the signal or whether the signal was transmitted in a valid manner. These comments do not take a position on whether the Global Privacy Control specification or the Global Privacy Control signal as communicated by any particular intermediary would or would not be a valid UOOM under the CPA. However, given the emerging complexity of the privacy signal landscape, the rules would be strengthened by accounting for the clear possibility that a valid UOOM becomes broadly implemented by an intermediary in a manner that is inconsistent with the requirements of the CPA.

In addressing this concern, the rules could provide encouragement that where practical, UOOMs permit identification of the transmitting mechanism (such as a specific browser, plug-in, or OS). With this modification in place, the Department could further strengthen the Rule 5.07 system for identifying valid UOOMs by identifying specific valid UOOM implementing mechanisms in addition to valid UOOM systems or standards. Finally, the rules could provide guidelines about the circumstances that would result in otherwise valid UOOMs being implemented in a legally deficient manner and the steps that a controller should take in response to a deficient UOOM in order to determine consumer intent.

C. Address the Unique Challenges Posed by "Do Not Sell" Lists that Operate as UOOMs

The draft rules provide that a valid UOOM will not necessarily function by communicating a signal, but may take other forms, such as an organization that maintains a queryable list representing the intent of consumers to invoke their CPA opt-out rights.[11] While this feature is not clearly contemplated by the Act and is not presently reflected in comparable state laws and rules that provide for the exercise of consumer rights through signal mechanisms,[12] FPF is optimistic that such lists can serve as an important tool to support the exercise of consumer privacy rights. Nevertheless, establishing, maintaining, and using an opt-out of sale and/or targeted advertising list (UOOM list) will pose unique challenges that the Department should consider addressing in its final CPA rules in order to ensure their effective development and implementation.

UOOM lists will pose implementation challenges and carry inherent limitations that are distinct from signal-based UOOMs. This is partially due to the greater technical and procedural complexity that UOOM lists will entail. Whereas a business that receives a signal as a consumer accesses its webpage can apply the expressed preference to associated data and (if known) broader consumer account information, a UOOM list will require businesses to collect information from each consumer, query one-or more valid UOOM lists, and perform or trust the results of a matching process between the collected data and UOOM list information, all before implementing validly expressed privacy preferences. Furthermore, information submitted by a consumer to a UOOM list may have limited durability in effectiveness if a consumer or developer updates a product or rotates/randomizes particular identifiers.

---

[11] Rule 5.06(A)(2).

[12] *See* California Consumer Privacy Act (CCPA) § 1798.185(a)(19) & (20), Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CACPDPOM) Sec. 6(e).

Consumers, regulated entities, and organizations interested in establishing a valid UOOM list would benefit from additional clarity in the final rules concerning:

- Examples of the information that consumers may be asked to provide to UOOM lists to enable authenticated preference matching in the context of different technologies (websites, apps, smart tvs, connected devices, etc.).
- Whether UOOM lists will enable consumers to selectively adjust their preferences for particular covered entities as is the case with many of today's opt-out signal mechanisms.
- How the providers of UOOM lists will protect and limit disclosure of the information provided by individuals.
- Functionally, the procedures by which covered organizations will collect information from consumers and query UOOM lists.
- Whether distinct Rule 5.03 Notice and Consent disclosures will be necessary given the unique features and limitations of UOOM lists.

D. Clarify the Application of the Rules' "Notice and Choice" Protections for the Use of 'on by default" UOOMs

Notwithstanding the CPA's direction that UOOMs may not be a "default setting,"[13] draft Rule 5.04 provides that a UOOM may be set by default if transmitted by a tool that does not come pre-installed on a device and "[i]s marketed prominently as a privacy-protective tool or specifically as a tool designed to exercise a user's rights to opt out."[14] Given that marketing materials (either in paid-advertising campaigns or the disclosures associated with a product or service) that generally refer to protecting privacy may not contain any information pertinent to the operation of a UOOM,[15] this provision appears inconsistent with Rule 5.03's requirement that the provider of a UOOM provide specific consumer notices about the intended effect and limitations of the mechanism.

More broadly, in the modern marketplace, essentially all consumer-facing, data-enabled products market or make representations about their commitments to respecting consumer privacy to at least some degree. Therefore, it is difficult to see how the use of a particular product (especially a multi-purpose, multi-feature product, such as a web browser or operating system) that merely represents itself as "privacy-protective" can be objectively determined to "clearly represent[] the consumer's affirmative, freely given, and unambiguous choice" to invoke one or both of the CPA's relevant opt out rights.[16] Furthermore, a generally "privacy-protective" service that enables a UOOM signal by default without adequate consumer notice or choice could negatively impact consumers by opting individuals out of certain desired product features or rewards programs that involve data "sales" under the CPA.

---

[13] CPA § 6-1-1313(2)(c).
[14] Rule 5.04(B).
[15] The concept of "privacy" is notoriously contested and culturally dependent. *See e.g.,* Deirdre K. Mulligan, Colin Koopman, & Nick Doty, "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy," Philosophical transactions. Series A, Mathematical, physical, and engineering sciences (2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5124066/.
[16] CPA § 6-1-1303(5)(c).

In order to ameliorate these inherent tensions in the draft rules, FPF recommends that the Department at a minimum clarify the application of Rule 5.03 concerning notice and choice requirements for UOOMs to 'on by default' UOOMs envisioned under Rule 5.04(B).

2. "Dark Patterns"

The draft rules provide helpful specificity about design practices that will be considered in violation of the CPA's restrictions on the use of "Dark Patterns." FPF recommends that the Department consider the following modifications as it reviews the draft rules: (1) provide greater clarity about the range of interfaces and consumer interactions to which the Rule 7.09(C) prohibition on the use of "Dark Patterns" applies, (2) elaborate on the relationship between the "substantial effect" standard laid out in the CPA's definition of "Dark Patterns" with the nine principles described in draft Rule 7.09(B), and (3) address the relevance of designer intent in determining whether a design feature constitutes a "Dark Pattern."

A. Clarify the Intended Scope of the Rule 7.09(C) Prohibition on the Use of "Dark Patterns"

FPF urges the Department to clarify the intended scope of Rule 7.09(C)'s prohibition on "Dark Patterns."[17] The Colorado Privacy Act restricts the use of "Dark Patterns," defined to encompass a "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice" only in obtaining consumer consent where required under the Act.[18] However, draft Rule 7.09(C) can be read as establishing a comprehensive prohibition on "Dark Patterns," not only within the context of consent, but potentially in *any* interface or interaction between covered entities and consumers. This reading is supported by language in draft Rules 4.02 and 5.03 which forbid the use of "Dark Patterns" "as defined in C.R.S. § 6-1-1303(9) and prohibited by 4 CCR 904-3, Rule 7.09" in the context of exercising personal data rights and providing notice and choice in conjunction with the use of an UOOM.[19]

---

[17] Rule 7.09(C); "The use of Dark Patterns, as defined in C.R.S. § 6-1-1303(9), is prohibited."
[18] CPA § 6-1-1313(2)(c).
[19] Draft Rule 7.09(C)'s placement within Section 7 does not resolve this uncertainty. Section 7 is described in Rule 7.01(A) of the draft rules as "provid[ing] clarity on the requirements to obtain Consent, including the prohibition against obtaining agreement through the use of Dark Patterns." Rule 7.01(A) may indicate that the prohibition on the use of "Dark Patterns" in 7.09(C) only applies to "obtaining agreement through the use of Dark Patterns," but this is not definitive in the face of other ambiguities. For example, Rule 7.09(B) states that the nine design principles highlighted in Rule 7.09(B) apply to "user interface or choice architecture" design, which facially goes beyond the context of consent. While each principle itself includes language limiting that principle to the consent context (Rules 7.09(B)(1), (2), (4), (5), (7), and (8) address "[c]onsent choice options," Rules 7.09(B)(3) and (6) address consent flows, and Rule 7.09(B)(9) addresses "[c]onsent choice architecture"), it is unclear whether the seemingly broader "user interface" language impacts the scope of the principles, adding to the lack of clarity for entities attempting to interpret the scope of Rule 7.09(C).

As the text of the CPA only restricts the use of "Dark Patterns" in the context of obtaining consent, a decision to create a broader, general prohibition on “Dark Patterns” through the rules should be approached thoughtfully. There is a long history in Colorado consumer protection jurisprudence about what constitutes an unfair or deceptive act or practice, what constitutes adequate notice and disclosure, what is a reasonable amount of marketing and persuasion, and what crosses the line. For example, the Colorado Consumer Protection Act already prohibits unfair and deceptive acts and practices.[20] Under this authority, the Attorney General’s office recently settled claims with law care service Fit Turf after finding that the company had intentionally entered consumers into auto-renewing services without their consent.[21] Insofar as the prohibition on the use of “Dark Patterns” laid out in Rule 7.09(C) is intended to go beyond this traditional definition, broader consideration is needed to understand where and how this provision expands general consumer protection law.

Additionally, a general prohibition on “Dark Patterns” would go beyond how similarly situated states have proscribed “Dark Patterns” in their comprehensive privacy laws (which, when addressed, have been typically cabined to consent flows).[22] Such an expansion would raise substantial new compliance questions for UX designers building many different interfaces, including interfaces without relevancy for consumer privacy. For example, a general prohibition on the use of “Dark Patterns” could be construed as applying to (and prohibiting) messages or designs that highlight a new consumer product or feature, decisions to only accept certain types of payment options, and all manner of designs that do not involve consent for data processing or even the collection of user data.

In sum, while there are both policy and legal arguments that may counsel both for and against a regulatory expansion of the prohibition on “Dark Patterns” beyond the context of obtaining consumer consent pursuant to the CPA, the far-reaching impact that such an expansion would have on the market requires clarification in the draft rules about the intended scope of the Rule 7.09(C) restrictions on the use of “Dark Patterns.”

B. Clarify the Relationship Between the CPA’s “Substantial Effect” Standard and Rule 7.09(B)’s Design Principles

The draft rules would be strengthened by clarifying whether and how the “substantial effect” standard from the § 6-1-1303(9) definition of “Dark Patterns” applies to the nine design principles presented in draft Rule 7.09(B). As currently drafted, it is unclear whether contraventions of the Rule 7.09(B) principles are standalone violations or if they only rise to the level of illegality when they met the § 6-1-1303(9) standard of having the “*substantial effect* of subverting or impairing

[20] Colorado Consumer Protection Act, *Colo. Rev. Stat. § 6-1-101 et seq*.
[21] *Attorney General Phil Weiser announces Fit Turf will pay $125,000 for misleading consumers on automatic renewal services, unlawful telemarketing practices*, Colorado Attorney General’s Office (Sept. 23, 2020), https://coag.gov/press-releases/9-23-20/.
[22] *See, ex.* “. . . agreement obtained through use of dark patterns does not constitute consent.” California CCPA § 1798.140(h); “‘Consent’ does not include … (C) agreement obtained through the use of dark patterns. CACPDPOM Sec. 1(6).

user autonomy, decision-making, or choice" (emphasis added). The answer to this question is significant because it impacts whether the Rule 7.09(B) principles should be read as bright-line rules or as examples of circumstances to which the "substantial effect" standard might apply. For example, including language such as "we'll miss you!" in an interface that provides the option to revoke previously given consent may be interpreted as emotionally manipulative language, but it is also language that consumers likely are accustomed to ignoring.

C. Address the Relevancy of Designer Intent in Evaluating Whether an Interface Constitutes a "Dark Pattern"

FPF recommends that the Department's final rules clarify whether and how designer intent factors into an analysis about whether an interface constitutes a "Dark Pattern." Recent modifications to draft implementing regulations for the California Consumer Privacy Act provide that designer intent is a "a factor to be considered" in "Dark Patterns" analysis, raising the question of whether this is also the case in other states with comparable legislation, including Colorado.[23]

There are strong reasons to consider designer intent as relevant (although not dispositive) in determining whether a particular design rises to the level of a "Dark Pattern." An intent analysis could help distinguish accidental "Dark Patterns," or even simply a poorly executed UX experience, from "Dark Patterns" designed or manipulated for the purpose of leading consumers to act outside of their best interests. Furthermore, an intent analysis would, where appropriate, allow covered entities to avoid strict liability in the event of a broken link, platform interference from a hostile actor, or other circumstances outside of an organization's reasonable control.

Simultaneously, there are compelling reasons why designer intent should not be controlling in a "Dark Patterns" analysis. First, there are evidentiary issues with determining and demonstrating proof of designer intent. Second, the potential automation of design, or certain aspects of design, may make designer intent less relevant going forward. Finally, because the primary concern with the use of manipulative design is consumer harm, an outcome-oriented approach should be the crux of any inquiry into the use of manipulative design.

3. Biometric Data

The Future of Privacy Forum applauds Colorado policymakers for establishing new protections for the use of biometric-based technologies, which can carry significant privacy risks when used to uniquely identify an individual. We further welcome the Department's decision to define relevant terms in the CPA rules. Given that the the draft rules' proposed definitions of "Biometric Data" and "Biometric Identifiers" do not precisely align with the use of those terms in others statutes or contexts, and in light of the significant impacts the definitions will have on individuals

[23] California Privacy Protection Agency, "Modified Text of Proposed Regulations" (Nov. 3, 2022) § 7004(c), https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf.

and businesses in Colorado, we highlight the following points of emphasis regarding the practical impact of these terms.

A. The Proposed Definitions May be Over-Inclusive

The draft rules distinguish between "Biometric Identifiers" and "Biometric Data," the former of which does not require that covered information be used or intended to be used for identification purposes.[24] While comparable U.S. state biometric and comprehensive privacy laws have different definitions of "Biometrics," a common denominator is that an entity uses the information for identification purposes.[25] This framework focuses on physiological data unique to a person which allows an entity to singly identify or verify the individual's identity. These definitions are rooted in this concept of uniqueness because, unlike other forms of sensitive personal data, when data physiologically unique to an individual is compromised or misused, there are very specific and innate privacy and security risks.[26] This approach is also reflected across technical, health, and government fields, which typically view "Biometric Data" as an inherently identifying trait unique to an individual.[27]

Under the definition of "Biometric Identifiers" in the draft rules, the CPA's coverage could extend to forms of behavioral and body-based data that is neither unique to a person nor used or intended to be used for identification purposes. In contrast to Biometric Identifiers like fingerprints or facial templates, many other forms of behavioral and body-based data are generally not uniquely identifying. For example, an iPhone camera may detect an individual's face to focus the lens, an inward-facing camera in a VR device may track a user's gaze to improve graphics, or a connected vehicle may monitor a drivers' eyes to ensure they are not falling asleep at the wheel. The body-based data in these scenarios is not uniquely identifying the individual, but rather detecting or characterizing them.[28] These processing operations pose different risks from those raised by identification and verification, and are more likely to pose privacy threats when used to generate sensitive inferences about a person.

---

[24] Rule 2.02.

[25] *See, e.g.* Illinois Biometric Information Privacy Act, 740 ILCS 14; Wash. Rev. Code Ann. §19.375.020; CCPA §1798.140(c); Virginia Consumer Data Protection Act §59.1-571.

[26] For example, the Illinois Biometric Privacy Act states: "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. *Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.*" (emphasis added).

[27] *See, e.g.,* definitions set forth by the National Institute of Science and Technology (NIST), https://www.nist.gov/programs-projects/biometrics; National Center for Biotechnology Information (NCBI), https://www.ncbi.nlm.nih.gov/books/NBK219892/; Federal Bureau of Investigation, https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/biometricschallenge2011.pdf; and the Department of Homeland Security, https://www.dhs.gov/biometrics.

[28] *See*, Tatiana Rice, "When is a Biometric No Longer a Biometric?" Future of Privacy Forum (May 19, 2022), https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric/.

Given these considerations, FPF recommends a deeper consideration of the unique risks and differences in potential harms posed by information falling under "Biometric Data" and "Biometric Identifiers" as presently defined in order to ensure that the regulatory approach taken best serves the intention of the CPA.

B. Clarify the Inclusion or Exclusion of DNA, Genetics, and Health Information

It is unclear whether and to what extent the draft rules' definitions of "Biometric Identifiers" or "Biometric Data" include DNA, genetic data, or "protected health information" as defined in the CPA. There is a growing divide in Biometric Data privacy laws (and comprehensive data privacy laws regulating biometrics) on the inclusion of DNA, genetic information, and health information within the definition and regulation of that which is a "Biometric."[29] It is rational to interpret Biometric Data's basic definition as a unique physiological characteristic to include distinctive health data. However while some health data such as DNA, heartbeat, or vein pattern can uniquely identify an individual, other forms of health data may not. Instead, like behavioral biometrics, other forms of health data may only be used for characterization and diagnosis, which may pose distinct privacy risks when used to generate sensitive inferences.

Additionally, because the Health Information Portability and Accountability Act (HIPAA) governs health information for patient settings but does not extend privacy protections to consumer-facing technologies like fitness trackers or reproductive health applications, there is considerable reason to ensure that health information, both uniquely identifying and those used for diagnostic purposes, is clearly defined in the statute. Therefore, in considering the appropriate scope of "Biometric Data" or "Biometric Identifiers," the final rules should address whether health information is excluded, and if so, how it otherwise fits within the CPA.

4. Children's Data

FPF welcomes the attention that both the CPA and the draft rules pay to protecting the privacy of children's personal information. Two brief clarifications would support the Department's goals. First, Rule 6.10(B) describes the rules for collecting sensitive information without consent for users "over the age of thirteen (13)." Since children are defined in CPA 6-1-1303(4) as "under thirteen years of age," it is not clear how to process sensitive data on 13-year-olds and whether it could be done without consent. If the intent was for 6.10(B) to cover this group, it should say "the age of thirteen (13) or over."

Second, the draft rules contain language that appears similar to the federal Child's Online Privacy Protection Act (COPPA), but it is not clear that the same definitions will be followed. Since the Colorado Attorney General can enforce both COPPA and these rules, further clarifications would help stakeholders understand how the Colorado Attorney General will enforce actions. The most

[29] *Compare, e.g.* Illinois Biometric Information Privacy Act, 740 ILCS 14; with New York §106-B, https://www.nysenate.gov/legislation/laws/STT/106-B.

noteworthy term to define in the draft rules is “directed to children.” This term is defined in detail in 16 CFR § 312.2 of the COPPA rule, but it isn’t clear if the Colorado Attorney General will follow the same standard in making determinations.

***

Thank you for this opportunity to provide input on Colorado Privacy Act rulemaking. We look forward to participating in the upcoming stakeholder sessions and look forward to future opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments, please contact Keir Lamont at klamont@fpf.org.

Sincerely,

Keir Lamont
Senior Counsel

Tatiana Rice
Policy Counsel

Felicity Slater
Policy Fellow