FUTURE OF
PRIVACY
FORUM

July 12, 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 Colorado Privacy Act pre-rulemaking comments

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

The Future of Privacy Forum (FPF) welcomes this opportunity to weigh in on pre-rulemaking considerations for the Colorado Privacy Act (CPA). 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 regulation.[1]

In response to the Department's targeted questions for informal input,[2] we offer resources and recommendations below regarding: universal opt-out mechanisms, consent, data protection assessments, consumer rights with respect to profiling, and biometric data. Our comments are directed toward: (1) ensuring the protection of individual privacy interests and the effective exercise of new consumer privacy rights under the CPA, (2) maximizing clarity and ease of understanding for business and nonprofit compliance efforts, and (3) promoting interoperability with emerging U.S. and global privacy frameworks where appropriate, particularly where the CPA adopts consistent substantive definitions and language as other jurisdictions.

Regulations promulgated under the Colorado Privacy Act should:

1. Clarify the approval and role of universal opt-out mechanisms in the context of today's labyrinth of existing permission frameworks, including in non-authenticated interactions and their application to off-site data.
2. Ensure that the CPA's high standard for obtaining valid consumer consent is realized in practice by providing that consent must be freely revocable and establishing limits on inappropriate "bundling" of consent for disparate processing purposes.

[1] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.
[2] Colorado Department of Law, "Pre-rulemaking considerations for the Colorado Privacy Act" (Apr. 2022), https://coag.gov/app/uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy-Act.pdf.

3. Provide appropriate guidance, flexibility, and interoperability for conducting meaningful data protection assessments, informed by best practices developed by regulators in both U.S. and global jurisdictions with comparable requirements.
4. Establish that a broad range of “profiling” decisions will be subject to consumer opt-out rights and follow best practices for interpretability of automated decision-making so that Coloradans are fully empowered to exercise their rights.
5. Adopt a definition of “biometric data” that protects individual privacy interests by limiting invasive and non-consensual tracking and identification.

1. Universal Opt-Out Mechanisms

Given the ever expanding range of digital products and services that consumers routinely interact with, data protection regimes that are rooted in establishing individual choices and controls over personal information collection and processing preferences will inevitably be overwhelming and unmanageable for ordinary people in practice.[3] The CPA represents a significant step forward for U.S. privacy law because it not only establishes important individual rights and protections, but provides that the rights to restrict targeted advertising and sales of personal data may be exercised through “user-selected universal opt-out mechanism[s].”[4] The effective development and deployment of such ‘privacy preference signals’ can enable consumers to exercise their rights on an automated basis, significantly easing the burdens of privacy self management.

Despite longstanding stakeholder efforts, at present, universal opt-out mechanisms remain a nascent concept in U.S. privacy law.[5] As the first state to unambiguously establish the ability for consumers to exercise privacy rights through technological preference signals, Colorado has an important opportunity to establish principled rules and guidance that will drive the effective development and adoption of preference signals while promoting harmonization of consumer rights across state borders. Multiple factors including the broad range of modern technologies that collect and process consumer data, the existing labyrinth of user-consent mechanisms, and fragmenting U.S. privacy legal landscape give rise to various outstanding technical and policy questions that must be resolved in order to ensure the effective deployment of universal opt-out mechanisms. Consumers and covered entities alike will benefit from additional certainty for how opt-out preferences signals are to be exercised and implemented.

As universal opt-out mechanisms are central to the intended operation of the CPA and are the only topic on which the CPA *requires* the adoption of rules, FPF recommends that the

[3] *See e.g.*, Woodrow Hartzog, *Prepared Testimony before the Senate Commerce Committee* (Feb. 27, 2019), https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53.
[4] Colorado Privacy Act (“CPA”) § 6-1-1306(1)(a)(IV)(B).
[5] *See* Maximilian Hils, Daniel W. Woods, & Rainer Böhme, “Privacy Preference Signals: Past, Present and Future” Proceedings on Privacy Enhancing Technologies (June 15, 2021), https://arxiv.org/pdf/2106.02283.pdf.

Department's initial rulemaking activity prioritize drafting regulations that will ensure predictable and effective exercise of preference signals. Addressing the following issues will help to ensure that users will be able to confidently exercise their new CPA privacy rights through opt-out mechanisms.

A. Prioritize consumer choice in the development of 'universal opt-out mechanisms'

The Colorado Privacy Act directs the Attorney General to adopt rules for opt-out mechanisms that are not "default setting[s]" but rather "clearly represents the consumer's affirmative, freely given, and unambiguous choice" to exercise individual privacy rights.[6] We note that this is a high standard for choice, substantially aligned with the Act's strong, four-part definition of "consent" (defined as "a *clear, affirmative* act signifying a consumer's *freely given*, specific, informed, and *unambiguous* agreement…" (emphasis added)).[7] As a result, regulations establishing requirements for valid universal opt-out mechanisms are required to ensure that consumer choice is central to the enabling of any specific preference signal. In some cases, this standard may conflict with privacy maximizing outcomes (certain signals may be legally ignored), but will uphold other policy goals, such as individual autonomy and preventing these mechanisms from becoming a tool leveraged by intermediary businesses seeking to block competitors' access to data.[8]

The Department's Request for Comment asks whether "a tool that is marketed for its privacy features" or "a privacy-focused version of a tool offered in multiple versions" would meet the requirements for consumer choice in exercising privacy rights through a universal opt-out mechanism.[9] In many cases, this will require a context-specific assessment of how a particular opt-out mechanism is implemented. For example, a consumer's installation of an on-by-default single-purpose browser plug-in that is explicitly marketed as a tool to exercise consumers' Colorado opt-out rights would certainly satisfy the CPA's requirements of consumer choice. On the other hand, the installation of a plug-in that has a different primary purpose (such as a password manager, screen reader, or user-interface add-on) that incidentally sends opt-out signals by default would probably not meet this standard.

In general, it is unlikely that a browser, operating system, or multi-purpose device that markets itself as generally protective of individual privacy that enables a Colorado-specific opt-out signal on behalf of its users would meet the Act's statutory requirements that signal mechanisms reflect unambiguous choice and are not default settings. In general, such products are marketed based on a wide variety of factors including protecting privacy, but also dimensions such as speed, user

[6] CPA § 6-1-1313(2)(c).

[7] CPA, § 6-1-1303(5).

[8] *See* CPA § 6-1-1313(2)(a) ("The rules must… not permit the manufacturer of a platform, browser, device, or any other product offering a universal opt-out mechanism to unfairly disadvantage another controller").

[9] "Pre-Rulemaking Considerations," *supra* note 2 at 3.

interface design, security, and safety features.[10] It would be impraticable to infer, from objective factors, that an individual has unambiguously chosen to use a particular, multi-purpose product due to its Colorado-specific opt-out signal features.

Meanwhile, an organization that receives a particular opt-out signal may not be able to determine the specific source or transmitting mechanism of the signal (for example, whether the signal came from a user's browser, specific plug-in, device setting, or other tool). In such cases, the signal source is relevant because the same specification or signal could be implemented by providers in ways that either do or do not meet the CPA's consumer choice requirements. If the same signal is widely implemented in a mix of both valid and invalid ways (some with consumer choice and others enabled by default), it could threaten the Attorney General's ability to enforce the law. On the other hand, the non-compliant implementation of a small percentage of the total signals for a specific, widely used opt-out mechanism should not provide a justification for covered entities to ignore all such signals. Overall, this dynamic calls for continued regulatory oversight and for the Attorney General to establish an open, authoritative process to review and approve valid opt-out signals as they mature and are implemented over time (as described below).

B. Clarify the application of 'universal opt-out mechanisms' in non-authenticated interactions and to off-site data

Forthcoming regulations should clarify the extent to which opt-out preference signals apply in the context of (1) non-authenticated interactions and (2) to information collected by a business or nonprofit separate from a consumer's present interaction.

The regulations should specify that an opt-out signal associated with less readily identifiable information can only apply to consumer information with which the signal can be *reasonably* linked. For example, when a customer who has an account with a business logs-in to a business website, that company can be expected to associate that browsing session with the consumer's account, including prior purchases, payment details, contact information, and other information that the individual has previously shared (including at an in-person store). However, if the individual visits the same website without logging into their account, the business may only have access to that individual's browser information - such as an IP address, cookie IDs, and other header information. While covered entities should clearly respect opt-out choices with respect to data directly associated with a signal, different businesses either may or may not be able to connect signals received in non-authenticated interactions with other customer information. Given that organizations may choose not to develop systems capable of associating non-authenticated browsing information with specific customer accounts, regulations should incentivize good faith privacy-protective design choices by establishing that honoring opt-out

[10] *See e.g.*, Michael Muchmore, "Edge, Firefox, Opera, or Safari: Which Browser is Best?" PC Mag (Apr. 4, 2022), https://www.pcmag.com/picks/chrome-edge-firefox-opera-or-safari-which-browser-is-best.

signals does not require covered entities to take additional, identifying steps to combine or link separate sources of personal information.

In circumstances where an opt-out preference signal sent through a browser or similar technology platform can be reasonably linked to other information associated with an individual collected in different contexts (such as offline data and information used in separate lines of business), a secondary question arises as to whether the signal request should apply to such data. For example, a user who has enabled a browser-level opt-out signal may be most concerned with avoiding online targeted advertising and may not intend for the signal to end their participation in a customer loyalty or rewards program that involves data "sales" under the CPA. On the other hand, if a user who enables opt-out signals finds that a purchase made in a physical store has been used to serve them advertising online they may be surprised or distressed. Recently proposed implementing regulations for the CPRA have addressed this issue by providing that if an opt-out signal conflicts with a consumer's prior participation in a financial incentive program, the business shall notify the consumer and ask whether they intend to withdraw from the program.[11]

Clarifying the role of opt-out mechanisms and respecting consumer expectations can also be supported through regulations that provide further guidance to the providers of particular preference signals for clearly describing the specific privacy choices that their mechanisms will communicate as well as their intended scope and effects.[12]

C. Address conflicts between universal opt-out mechanisms and other expressions of consumer choice

Consumers today face an expanding labyrinth of privacy options across different platforms, technologies, and organization-specific privacy settings.[13] Forthcoming rules should give further clarification as to how covered entities that receive valid universal opt-out signals should balance these requests against other forms of consent for targeted advertising and data sales (obtained through mechanisms such as through cookie banners, privacy dashboards, and similar tools). The CPA addresses potential conflicts by providing that consumer consent offered through a "web page, application, or similar method" may take "precedence over any choice reflected through the universal opt-out mechanism."[14]

[11] California Privacy Protection Agency, "Text of Proposed Regulations" §7025(4)(4)(C), *available at* https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf

[12] *See* CPA § 6-1-1313(2)(d).

[13] A diverse array of consumer privacy signals already exist, including browser and device-specific privacy settings (to block cookies, block third-party cookies, "prevent cross-site tracking"); browser plug-ins; global signals such as Do Not Track and the Global Privacy Control; and self-regulatory mechanisms such as the NAI Consumer Opt Out and DAA YourAdChoices. Similarly, control over mobile apps can be exercised through device settings (iOS and Android), including "Limit Ad Tracking," and app-specific permissions.

[14] CPA § 6-1-1306(1)(a)(IV)(C).

The Department should consider additional guidance to uphold the CPA's strong definition of "consent" in this context. Specifically, the use of cookie banners or similar website notification banners that seek consent for third-party sales or targeted advertising that would override a qualifying opt-out signal should be scrutinized to ensure such consent is valid. Regulatory guidance or illustrative examples should affirm that consent obtained through cookie banners should not be implied (through inaction, closing a banner, or scrolling down), or achieved through non-symmetrical choices (such as only offering consumers with buttons of "accept all" and "more options," the latter of which leads to a multi-step process to decline). As a legal matter, such a consumer-friendly approach is consistent with the CPA and would be interoperable with emerging regulations in California.[15] As a policy matter, it will disincentivize over-reliance on cookie banners, which have emerged as a significant user complaint in the implementation of Europe's data protection rules.[16]

D. Establish an open process for the authoritative approval of qualifying 'universal opt-out mechanisms' over time

In the fragmented consumer data ecosystem of web, mobile, screenless IoT, connected vehicles, and other emerging technologies, it is unlikely that a single, truly "universal" opt-out mechanism will be developed that can effectively apply across all digital (and physical) contexts in which a consumer interacts with businesses and non-profit organizations. For example, a browser signal or plug-in might be best suited for communicating opt-out choices to websites, while a separate mechanism might better express consumer choice while using apps. Consequently, a range of different context (and legal regime)-specific preference signals are likely to be developed and refined over time to be exercised through various mediums including apps, browsers, plug-ins, and operating systems. In this environment, consumers need to have confidence that the specific signals they choose to enable will have legal effect and covered entities will require direction for detecting and implementing the qualifying opt-out preference 'signals in the noise.'

One option for promoting clarity would be for CPA regulations to point to specific opt-out signal protocols or specifications as exemplars.[17] However, given that forthcoming regulations and new technologies and business practices will drive the continued development of a variety of context-appropriate mechanisms beyond presently existing consumer options, specific signals favored by regulations could quickly become outdated while superior, future mechanisms would lack clear force of law. Instead, regulations should adopt principled criteria for qualifying mechanisms (as described above) and the Attorney General's Office should establish an open,

[15] *See e.g.*, Proposed CPRA Implementing Regulations *supra* note 11 § §7004(a)(2)(C) ("A website banner that serves as a method for opting out of the sale of personal information that only provides the two choices, "Accept All" and "More Information," or "Accept All" and "Preferences," is not equal or symmetrical…").

[16] *See e.g.*, Joe Nocera, "How Cookie Banners Backfired" The New York Times (Jan. 29, 2022), https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html.

[17] *See* "Pre-Rulemaking Considerations", *supra* note 2 at 2.

authoritative process for the ongoing review and approval of universal opt-out mechanisms that adhere to the CPA's requirements and implementing regulations. Such a process could take the form of interpretive guidance, enforcement opinion letters on presumptively valid opt-out tools, public workshops, and/or public comment periods on proposed opt-out tools. In approving qualifying mechanisms, we recommend that the Agency consult with technical, legal, and policy experts, as well as regulators in other jurisdictions that are reviewing similar tools, such as California and Connecticut.[18]

2. Consent

The Colorado Privacy Act establishes a strong, four-part test for valid consent, comparable to leading U.S. state and global privacy regimes, including the California Privacy Rights Act ("CPRA"), the Virginia Consumer Data Protection Act ("VCDPA"), the Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("CTDPA"), and the European Union's General Data Protection Regulation ("GDPR").[19] The requirement that consent be freely given, specific, informed, and unambiguous will clearly invalidate purported consent obtained through the use of deceptive and manipulative user-interface design practices commonly referred to as "dark patterns," regardless of how potential rulemaking on that topic proceeds. However, in order to uphold this high standard for consent in the operation of the CPA, we recommend that regulations affirm two additional aspects of consent that are already implicit in the Act: (1) consent must be freely withdrawable, and (2) consent for unnecessary secondary purposes should not be "bundled" with consent for processing that is central to providing a product or service.

A. Regulations should clarify that a consumer may freely withdraw consent for processing at any time

FPF recommends that forthcoming regulations clarify that consumers have the right to withdraw previously provided consent for the processing of sensitive personal information or the use of data for inconsistent secondary purposes under the CPA. The Act appropriately recognizes that consent for targeted advertising and data sales that overrides universal opt-out mechanisms must allow a consumer to "revoke the consent as easily as it is affirmatively provided."[20] However, an equivalent right to withdraw or revoke consent is not explicitly made available in the CPA's definition of "consent" (§ 6-1-1303(5)) or provisions on consent for the processing of sensitive personal data (§ 6-1-1308(7)) or use of data for secondary purposes (§ 6-1-1308(4)).

[18] Connecticut Act Concerning Personal Data Privacy and Online Monitoring ("CTDPA") § 6(e)(1)(A)(ii) ; California Privacy Rights Act (CPRA) and California Privacy Rights Act ("CPRA") § 1798.135(b).

[19] The CPA's four-part requirement that valid consent must be: (1) freely given, (2) specific, (3) informed, and (4) unambiguous is mirrored by requirements in the CPRA § 1798.140(h), VCDPA § 59.1-571, CTDPA § 1(6), and GDPR Art. 4(11).

[20] CPA § 6-1-1306(1)(a)(IV)(C).

The ability to withdraw previously offered consent is recognized as a critical aspect of legitimately obtained consent in global privacy laws. Most notably, the GDPR's 'conditions for consent' provides that an individual shall "have the right to withdraw his or her consent at any time."[21] Guidance from the European Data Protection Board further clarifies that consent will not be considered to satisfy the "freely given" element if an individual is "unable to refuse or withdraw his or her consent without detriment."[22] Finally, the European Commission has specified that withdrawing consent requires that a controller "ensure that the data is deleted unless it can be processed on another legal ground."[23]

Given the alignment between the CPA's definitional approach to consent and the GDPR, it appears clear that the right to revoke consent is implicit under Colorado law, though some have suggested that U.S. courts may not be inclined to read such a requirement into the CPA.[24] Recently enacted privacy legislation in Connecticut, modeled closely on the Colorado Privacy Act, resolves this ambiguity by clearly providing that controllers shall:

> "[P]rovide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request."[25]

In order to ensure that consumer consent obtained pursuant to the CPA is freely given, FPF recommends that forthcoming regulations follow an approach similar as Connecticut by providing that consumers may, at any time, withdraw previously provided consent. In implementing a withdrawal, a controller and their processors should be obligated to delete or otherwise render permanently anonymized or inaccessible personal data at a reasonable time following the revocation.

B. The regulations should limit inappropriate 'consent bundling'

In order to ensure that consumer consent obtained pursuant to the Colorado Privacy Act is "specific," regulations should ensure that consent requests for significantly divergent collection and processing purposes are not inappropriately grouped into "take-it or leave-it" offers.

[21] GDPR Art. 7(3).

[22] EDPB, "Guidelines 05/2020 on consent under Regulation 2016/679," § 7.3 para. 164 (May 4, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[23] European Commission, "What if somebody withdraws their consent?", https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en (accessed on Jun. 6, 2022) *see also id*. at § 5.2 para. 117 & 118.

[24] *See e.g.*, David A. Zetoony, "Do people always have the right to withdraw consent?" Data Privacy Dish (Feb. 1, 2022), https://www.gtlaw-dataprivacydish.com/2022/02/do-people-always-have-the-right-to-withdraw-consent/.

[25] CTDPA § 6(6).

However, while regulations against consent "bundling" are appropriate, they should also be balanced so as not to result in overwhelming consumers with an unmanageable volume of consent requests. Regulations should avoid a regime that could lead to the development of user "consent fatigue" in which individuals receive so many requests for consent that they are disincentivized from meaningfully engaging with information regarding each particular choice.[26]

To do ensure that consent is "specific" and "freely given", regulations should clarify that consumers must be able to accept the processing of sensitive data for purposes that are central to securely and effectively providing a product or service pursuant to § 6-1-1308(7) separately from consent for data processing that is not reasonably necessary to or compatible with the specified purposes for processing § 6-1-1308(4). Again, lessons from the other jurisdictions that are implementing equivalent language on consent may be instructive on this topic.

In California, recently proposed implementing regulations for the CPRA address consent bundling by providing that businesses should obtain separate consent for "unexpected or incompatible" uses of personal information.[27] The European Data Protection Board also provides the following guidance:

> "[T]he situation of 'bundling' consent with acceptance of terms or conditions, or 'tying' the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given."[28]

The issue of consent bundling was directly addressed in a recent case pursued by the Norwegian Data Protection Authority (Datatilsynet) which found that "the sharing of location data with advertising partners for behavioural advertisement purposes was bundled with processing of location data for the *proper function* of the app, depriving the user of genuine *free choice*…"[29] (emphasis added). The Court of Justice of the European Union (CJEU) has also clarified in the Orange Romania ruling that "in order to ensure that the data subject enjoys genuine freedom of choice, the contractual terms must not mislead him or her as to the possibility of concluding the contract even if he or she refuses to consent to the processing of his or her data".[30]

Forthcoming CPA regulations could build out on the concept of consent that is necessary for "proper function" of a product or service versus consent that is necessary for unrelated incompatible and unexpected secondary uses of data.

[26] *See e.g.*, Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, & Thorsten Holz, "(Un)informed Consent: Studying GDPR Consent Notices in the Field," Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (Nov. 6, 2019), https://dl.acm.org/doi/10.1145/3319535.3354212.

[27] Proposed CPRA Implementing Regulations *supra* note 11 § 7004(A)(4)(C).

[28] EDPB Guidelines 05/2020 on consent, *supra* note 22, at § 3.1.2 para. 26.

[29] Datatilsynet, "Administrative fine - Grindr LLC," Case No. 20/02136-18 (Dec. 13, 2021), https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf.

[30] CJEU, Judgment of November 11, 2020, Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), C-61/19, ECLI:EU:C:2020:901, paragraph 41.

Resources:

- European Data Protection Board, "Guidelines 0/5/2020 on consent under Regulation 2016/679" (May 4, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
- Information Commissioner's Office, "What is valid consent?" https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/
- European Commission, "What if somebody withdraws their consent?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

3. Data Protection Assessments

The Colorado Privacy Act is one of four U.S. state privacy laws taking effect in 2023 that will require organizations to conduct and document assessments of high-risk data processing activities.[31] Data protection assessments are an important tool for ensuring that organizations consider privacy implications and safeguards in the development of products and services while also providing for a record that allows organizations to demonstrate compliance efforts.[32] Although data protection assessments have long been a feature of administrative governance in the United States,[33] U.S. consumer privacy laws have not historically mandated that private organizations conduct data risk assessments. As a result, both formal and informal regulatory guidance will be helpful to ensure that these assessments fulfill their intended purposes without creating unnecessary costs and procedural hurdles for covered entities.

A. Provide guidance that supports context-appropriate flexibility in developing and conducting data protection assessments

The risk assessment requirements under forthcoming U.S. state privacy laws contain substantially aligned provisions on processing activities that must be assessed, assessment content, and

[31] *See* CPRA § 1798.185(15)(B), VCDPA § 59.1-576, and CTDPA § 8.

[32] *See* Information Commissioner's Office, "Guide to Data Protection Impact Assessments, 'What is a DPIA?'", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/ (last accessed Jun. 29, 2022).

[33] *See* Revision of OMB Circular A-130, "Managing Information as a Strategic Resource," FR Doc. 2016-17872 (July 28, 2016), https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.

reporting requirements.[34] FPF recommends that forthcoming CPA regulations avoid prescriptive requirements on the form that risk assessments should take, which could bring these state provisions out of sync and result in organizations preparing duplicative, Colorado-specific assessments, which would increase compliance costs without obvious benefits to consumer privacy. Any forthcoming regulations should further ensure that organizations have appropriate leeway to seriously examine their data flows, associated risks, and mitigating safeguards and are not incentivized to treat assessments as a purely defensive or box-checking measure. A flexible approach will have the added benefit of supporting the development of sector-specific, context appropriate assessments best suited for particular types of data processing (e.g., targeted advertising and consumer scoring), and sensitive categories of data (e.g., health data and mobility information).[35]

B. Develop regulations and informal guidance informed by existing best practices for data protection assessments

Given that many organizations, especially small companies and nonprofits, will likely conduct data protection assessments for the first time as part of their CPA compliance operations, it may be appropriate for the Attorney General's Office to assemble a catalog of resources containing sample assessment templates and other informal guidance outside the regulatory process.

Requirements to conduct and document assessments of inherently risky data processing practices, risks, and mitigating safeguards are a common feature of modern global privacy laws.[36] To support compliance efforts, regulators in the United Kingdom, France, Spain, Singapore, and New Zealand have all developed extensive guidance documents and tools (available in English) to help organizations determine when to conduct assessments, key concepts that assessments must consider, and procedures for reviewing and updating assessments over time (see resources below). The Commission nationale de l'informatique et des libertés (CNIL), the French Data Protection Authority (DPA), has even developed software to assist organizations conducting DPAs.[37]

[34] *See generally*, Christian M. Auty & Goli Mahdavi, "Comparing the Data Protection Assessment Requirements Across the Next Generation of U.S. State Privacy Laws," BCLP Law (Nov. 30, 2021), https://www.bclplaw.com/en-US/insights/comparing-the-data-protection-assessment-requirements-across-the-next-generation-of-us-state-privacy-laws.html.

[35] *See e.g.*, Chelsey Colbert & Kelsey Finch, "FPF and Mobility Data Collaborative release resources to help organizations assess the privacy risks of sharing mobility data," Future of Privacy Forum (Aug. 30, 2021), https://fpf.org/blog/fpf-and-mobility-data-collaborative-release-resources-to-help-organizations-assess-the-privacy-risks-of-sharing-of-mobility-data/.

[36] *See e.g.,* GDPR Art. 35; General Personal Data Protection Law (Brazil) Art. 38; Personal Information Protection Law (China) Art. 56; Personal Data Protection Act (Singapore) Art. 14.

[37] CNIL, "The open source PIA software helps to carry out data protection impact assessment" (June 30, 2021), https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment.

FPF recommends that the Attorney General's Office develop guidance for conducting CPA-compliant assessments that are informed by existing requirements and best practices for data protection assessments, rather than create a new approach (such as drawing from assessments developed in different contexts such as environmental impact assessments or enterprise risk management).[38] This approach will allow Colorado organizations and consumers to benefit from high existing standards for data protection and promote harmonization with global privacy frameworks, a stated regulatory priority.[39]

C. Clarify "comparable" processing operations to ensure high-risk processing will be subject to assessment

Conducting data protection assessments can be a time- and resource-intensive process for organizations, so it is appropriate to ensure that when substantially similar processing activities pose consistent risks, organizations are not required to conduct duplicative assessments that would not provide for new analysis. Consistent with this principle, the CPA provides that a data protection assessment may "address a comparable set of processing operations that include similar activities."[40] The GDPR similarly provides that "[a] single assessment may address a set of similar processing operations that present similar high risks."[41] While this has not been a prominent issue in GDPR enforcement, guidelines from European data protection regulators state that "[a] single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks."[42]

Resources:

- Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" WP 248 rev.01 (Oct. 4, 2017), https://ec.europa.eu/newsroom/article29/items/611236
- Information Commissioner's Office [United Kingdom], "Sample DPIA Template" (Feb. 2018), https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf
- Commission nationale de l'informatique et des libertés (CNIL) [France] "GDPR Toolkit > Privacy Impact Assessments," https://www.cnil.fr/en/privacy-impact-assessment-pia
- Agencia Española de Protección de Datos (AEDP) [Spain], "Risk Management and Impact Assessment Regarding Data Protection" (June 27, 2022), https://www.aepd.es/en/areas/innovation-and-technology

[38] *Contra* "Pre-Rulemaking Considerations", *supra* note 2 at 4.
[39] *Id*. at 2.
[40] CPA § 6-1-1309(5).
[41] GDPR Art. 35(1).
[42] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA)" (Oct. 4, 2017), https://ec.europa.eu/newsroom/article29/items/611236/en, endorsed by the EDPB.

- Personal Data Protection Commission (PDPC) [Singapore], "Guide to Data Protection Impat Assessments" (Sept. 14, 2021), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/DPIA/Guide-to-Data-Protection-Impact-Assessments-14-Sep-2021.ashx?la=en.
- New Zealand Privacy Commissioner, "Privacy Impact Assessment Handbook" (July, 2015), https://www.privacy.org.nz/publications/guidance-resources/privacy-impact-assessment-handbook/

4. Profiling and "Legal or Similarly Significant Effects"

The Colorado Privacy Act provides consumers with a right to opt-out of the automated processing of personal data "for the purposes of … [p]rofiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."[43] In furtherance of this right, forthcoming rules can benefit from the experience of existing data protection regimes that incorporate equivalent language. Specifically, Article 22 of the GDPR protects data subjects from "decisions based solely on automated processing, including profiling which produces legal effects […] or similarly significantly affects him or her."[44] Similar questions to those faced by European regulators applying this provision are likely to arise during the enforcement of the CPA.

FPF recently released a report analyzing over 70 cases and data protection authority decisions interpreting and and applying the GDPR's application to Automated Decision Making (ADM), which includes "profiling."[45] Although the rights and obligations for organizations engaging in profiling differ between Colorado and the EU (with Colorado providing an opt-out right, rather than broader restrictions), the similarity in definition and scope of profiling can inform threshold CPA rulemaking questions about what profiling decisions will be subject to consumer opt-out rights.

A. Provide guidance on the definition of "legal or similarly significant effects" to ensure the broadest protection of individual rights

In promulgating rules or guidance on the types of profiling decisions that will be considered to have "legal or similarly significant effects," the Department should interpret the scope of decisions that "result" in the provision or denial of services and opportunities broadly to give the strongest possible protections for Colorado residents. The CPA appropriately defines these effects as those that "result[] in the provision or denial of financial or lending services, housing,

[43] CPA § 6-1-1306(a)(I)(C).

[44] GDPR Art. 22; Additional information on the European regulatory approach to profiling can be found in Recital 71.

[45] *See* Sebastião Barros Vale and Gabriela Zanfir-Fortuna, "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities," Future of Privacy Forum (May 23, 2022) https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services."[46]

Crucially, in-scope profiling should include the cumulative automated decisions that substantially *contribute* to the provision or denial these significant opportunities (so-called 'pipeline' decisions[47]), rather than only the final decisions. For example, in considering "employment opportunities," consumer rights should extend to automated profiling that elevates or scores resumes, evaluates "personality" or "fit," or makes predictions about future success, rather than narrowly applying to a final decision of whether to offer or terminate a job or contract. Employment "opportunities" should similarly be read broadly to include not just hiring decisions, but the availability of opportunities within the context of a particular job.

In addition to establishing strong protections for Colorado residents, this approach to profiling will also align with emerging interpretations of parallel provisions under the GDPR. For example, European regulators have paid particular attention to the legal standard for "significant" effects of profiling in the context of app- and gig-based work. Many of these services function by using profiling decisions that affect which workers are selected for a given opportunity. Significant cases include:

- *Foodinho*: The Italian DPA considered the determination of a driver's "score" used to assign certain food and product deliveries to be a significant effect because of how the score impacted income and employment opportunities.[48]
- *Ola*: An Amsterdam court found that a ride-share company's automated fare deductions or fines against its drivers based on collected performance data had "significant" effects under the law.[49]
- *Uber*: The same Amsterdam court separately found that the potential economic effects of an automated fraud signal that could temporarily lock driver accounts did not rise to a sufficient level of significance to warrant elevated protections due to a lack of "long term of permanent effect[s]".[50]

These cases demonstrate that the significance of profiling effects is a complex, fact-intensive issue that would benefit from additional clarity from Colorado rulemaking so courts and organizations can make consistent determinations. The rules could provide criteria for assessing

[46] CPA § 6-1-1303(10).

[47] Miranda Bogen & Aaron Rieke, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias," Upturn (Dec. 2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

[48] Garante per la protezione dei dati personali, Case 9675440 (June 10, 2021) *available at* https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9675440.

[49] Rechtbank Amsterdam, Case C/13/689705 (Mar. 11, 2021) *available at* https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/689705/HA_RK_20-258.

[50] Rechtbank Amsterdam, Case C/13/692003 (Mar. 11, 2021) *available at* https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/692003/HA_RK_20-302.

"similarly significant effects", such as (i) affecting the circumstances, behaviour or choices of the individuals concerned, (ii) having a prolonged or permanent impact on the data subject, or (iii) leading to the exclusion of or discrimination against individuals. Additionally, the rules could provide illustrative examples of edge cases to assist covered entities in understanding when their automated decisions are of sufficient significance to be subject to the CPA's requirements.

B. Ensure transparency requirements for profiling will provide meaningful information to consumers

Clarifying the requirements for covered entities to provide meaningful information to consumers about profiling activities that informs or results in decisions that produce legal or similarly significant effects will be vital to support consumers' opt-out rights.[51] Consumers will typically be best informed if provided with information about the factors that led to a high-impact decision and the main reasons for it, rather than divulging specific algorithms or source code, which can be difficult to interpret and implicate trade secrets.

FPF recommends drawing upon existing best practices for explainability in automated decision-making and profiling to clarify the categories and granularity of information that organizations should provide related to profiling decisions under the CPA. For example, the European Data Protection Board (EDPB) has endorsed guidelines that information provided to data subjects about automated decision-making under GDPR Articles 13(2)(f) and 14(2)(g) should include:

- The categories of data that have been or will be used in the profiling or decision-making process;
- Why these categories are considered pertinent;
- How any profile used in the automated decision-making process is built, including any statistics used in the analysis;
- Why this profile is relevant to the automated decision-making process; and
- How it is used for a decision concerning the data subject.[52]

In 2021, the Italian Supreme Court applied these guidelines in a case against the Associazione Mevaluate Onlus, finding that it was necessary that users be informed about the "executive scheme," or the logic involved, and the constitutive elements of the 'reputational rating' algorithm at issue in order to meet the GDPR transparency obligations and to enable properly informed consent from data subjects.[53] In another 2021 holding, the Spanish DPA found that a bank had failed to gain appropriate consent for client profiling practices due by failing to properly inform its

[51] The CPA's duty of transparency does not provide explicit rules for disclosing information in the context of profiling, making this an appropriate topic for rulemaking. *See* CPA § 6-1-1308(1)(a).

[52] *See* EDPB/WP29, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/items/612053/en.

[53] Corte Suprema de Cassazione, Civile Ord. Sez. 1 Num. 14381 (May 25, 2021) *available at* https://gdprhub.eu/index.php?title=Cass.Civ._-_14381/2021.

clients “about the types of profiles it intended to build, their specific uses and consequences, [and] about the individuals’ right to object.”[54]

Regulations governing transparency of profiling operations should be further informed by the National Institute of Standards and Technology’s (NIST) interpretability guidelines for explainable artificial intelligence. These principles describe how explainable systems should (1) provide an explanation; (2) be understandable to its intended end-users; (3) be accurate; and (4) operate within its knowledge limits, or the conditions for which it was designed.[55]

C. Clarify how the Colorado Privacy Act applies to profiling decisions subject to different degrees of human oversight

In developing regulations on profiling and automated decisions, FPF recommends clarifying under what conditions human involvement and oversight means that profiling has not been carried out on an “automated” basis (and would thus not be subject to opt-out rights). Where human review of a profiling decision amounts to little more than a “rubber stamp,” the rules should clearly preserve the consumer’s opt-out rights. Specifically, regulations should clarify that a human nominally making a final determination or implementation does not render profiling as not automated. Instead, meaningful human involvement should require consideration of available data as well as the authority and competency to change outcomes.

Furthermore, the EDPB has clarified that the GDPR’s definition of profiling under Article 4(4) - refers to ‘any form of automated processing’ rather than ‘solely’ automated processing”. Therefore, “Profiling has to involve some form of automated processing – although human involvement does not necessarily take the activity out of the definition.”[56] This underlines the need for clarifying the meaning of “automated” in the definition of profiling through regulations, as well as the degree of human involvement that would exclude certain evaluations, analyses or predictions about data subjects from the scope of the definition and, therefore, of the right to opt-out.

For example, in the GDPR context, the Portuguese DPA reviewed a university’s use of proctoring software to analyze students’ behavior during exams to build a fraud likelihood score. The analysis would then inform the final human-made decisions (by professors) on whether to invalidate students’ exams or not. Such decisions were found to be fully automated despite

[54] AEPD, Procedimiento Nº: PS/00477/2019 (Jan. 13, 2021) *available at* https://gdprhub.eu/index.php?title=AEPD_-_PS-00477-2019.

[55] P. Jonathon Phillips et. al, “Four Principles of Explainable Artificial Intelligence,” U.S. Department of Commerce, National Institute of Standards and Technology (Aug. 2020), https://www.nist.gov/system/files/documents/2020/08/17/NIST%20Explainable%20AI%20Draft%20NISTIR8312%20%281%29.pdf.

[56] *See* European Data Protection Board, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, p. 7 (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/items/612053/en.

professors making the final decision as to whether to conduct an investigation and ultimately on whether to invalidate the exam. The Court determined that the lack of "guiding criteria" for evaluating the automated scores could "generate situations of discrimination and lead teachers to validate the systems' decisions as a rule."[57]

Resources:

- Sebastião Barros Vale and Gabriela Zanfir-Fortuna, "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities," Future of Privacy Forum (May 23, 2022), https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf
- P. Jonathon Phillips et. al, "Four Principles of Explainable Artificial Intelligence," U.S. Department of Commerce, National Institute of Standards and Technology (August 2020), https://www.nist.gov/system/files/documents/2020/08/17/NIST%20Explainable%20AI%20Draft%20NISTIR8312%20%281%29.pdf
- European Data Protection Board, EDPB/WP29, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01)" (February 6, 2018), https://ec.europa.eu/newsroom/article29/items/612053/en.
- Rebecca Crootof, Margot Kaminski, & W. Nicholson Price II, "Humans in the Loop" Vanderbilt Law Review (Forthcoming 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4066781.
- Aaina Agarwal, Patrick Hall, Sara Jordan, and Brenda Leong, "Five Things Lawyers Need to Know About AI," Future of Privacy Forum (October 2021), https://fpf.org/blog/five-things-lawyers-need-to-know-about-ai/
- Future of Privacy Forum, "The Privacy Expert's Guide to Artificial Intelligence and Machine Learning" (October 2018), https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

5. Biometric Data

The Colorado Privacy Act provides that "biometric data that may be processed for the purpose of uniquely identifying an individual" is a category of "sensitive data" subject to the Act's consent requirements.[58] FPF recommends that forthcoming regulations develop a clearly scoped definition of "biometric data" that protects individual privacy interests and provides clarity to organizations.

Biometric information that relies on biological or physical attributes is inherently sensitive because such data cannot typically be changed by individuals and can give rise to significant

[57] CNPD, Deliberação n.º 2021/622 (May 11, 2021) *available at* https://gdprhub.eu/index.php?title=CNPD_(Portugal)_-_Delibera%C3%A7%C3%A3o/2021/622.
[58] CPA § 6-1-1303(24)(b).

risks, such as identity theft, if lost or misused. At the same time, without further clarification, the term “biometric data” could arguably encompass a broad range of data including mere photographs and audio records (not subject to any further, identifying processing such as generating a ‘faceprint’) that would implicate First Amendment protections if covered by the CPA.[59] Of the five states that have enacted comprehensive privacy laws, all but Colorado have sought to avert such issues by establishing clear definitions of “biometric” information.[60]

If “biometric data” is not defined under the CPA, regulated entities may look to the definition of “biometric data” under Colorado’s security breach notification law which narrowly applies only to information collected for the purpose of authenticating an online account.[61] This definition would exclude data processing practices that give rise to many of the privacy and security concerns about the commercial collection use of biometric data, including 1:many facial recognition identification and persistent tracking.

FPF recommends adopting a definition that would clearly limit invasive, identifiable tracking of individuals over time without their consent, while clearly excluding categories of data (such as photographs and videos) that have not been processed to allow for unique identification. For example, a reasonable definition of “biometric data” can be found in Connecticut’s recently enacted comprehensive privacy law:

> “‘Biometric data’ means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include (A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.”[62]

Resources:

- 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/
- Brenda K. Leong, “Understanding Facial Detection, Characterization and Recognition Technologies,” Future of Privacy Forum (Mar. 2018), https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf

[59] *See e.g.*, Bill Kenworthy, “Photography & First Amendment” Freedom Institute (Apr. 2012), https://www.freedomforuminstitute.org/first-amendment-center/topics/freedom-of-the-press/photography-first-amendment.

[60] CPRA § 1798.140(c); VCDPA § 59.1-571; CTDPA § 1(3); Utah Consumer Privacy Act § 13-61-101(6).

[61] C.R.S. § 6-1-716(1)(a).

[62] CTDPA § 1(3).

***

Thank you for this opportunity to provide input on initial rulemaking under the Colorado Privacy Act. We welcome any further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Keir Lamont at klamont@fpf.org.

Sincerely,

Keir Lamont
Daniel Sturkie