epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

COLORADO DEPARTMENT OF LAW

On Proposed Rulemaking Under the Colorado Privacy Act of 2021

August 5, 2022

---

The Electronic Privacy Information Center ("EPIC") is a public interest research center based in Washington, D.C., that was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values.[1] EPIC has a long history of promoting transparency and accountability for information technology.[2]

EPIC submits these comments in response to the Colorado Department of Law's (hereinafter "Department") call for input on the rulemaking associated with the Colorado Privacy Act ("CPA").[3] We support the efforts of the Department to establish robust, pathbreaking privacy protections for Coloradans.

The state of privacy legislation and regulation in the United States is a patchwork of overlapping but non-identical requirements that are frequently shifting as new developments and technologies come to the fore. As the Department finalizes regulations, we urge you to lead in

---

[1] EPIC, *About EPIC* (2022), https://epic.org/about/.

[2] Comments of EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf. Comments of EPIC, https://epic.org/epic-recommends-cfpb-strengthen-buy-now-pay-later-bnpl-market-inquiry-on-customer-acquisition-and-data-practices/ Comments of EPIC, Implementation Plan for a National Artificial Intelligence Research Resource (Oct. 1, 2021), https://epic.org/documents/request-for-information-rfi-on-an-implementation-plan-for-a-national-artificial-intelligence-research-resource/ EPIC, *Algorithmic Transparency* (2018), https://www.epic.org/algorithmic-transparency/; EPIC, *Algorithms in the Criminal Justice System* (2018), https://www.epic.org/algorithmic-transparency/crim-justice/; Comments of EPIC, *Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics*, Federal Trade Commission (Aug. 20, 2018), https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-20-2018.pdf; Comments of EPIC, *Developing UNESCO's Internet Universality Indicators: Help UNESCO Assess and Improve the Internet*, United Nations Educational, Scientific and Cultural Organization ("UNESCO") (Mar. 15, 2018), 5-6 https://epic.org/internetuniversality/EPIC_UNESCO_Internet_Universality_Comment%20(3).pdf.

[3] https://coag.gov/resources/colorado-privacy-act/.

the protection of consumer rights, consistent with the will of Colorado voters. The Department should prioritize regulations that clearly articulate the scope and nature of individual privacy rights and the responsibilities imposed on entities that collect personal information. The rules should clearly define the scope of the CPA and identify specific forms of data collection, processing, and transfer that are permitted or prohibited. EPIC urges the Department to draft rules that would:

- Set out clear standards for personal data collection, use, and transfer that restrict behavioral tracking and secondary uses of data (Page 2);
- Broadly define "dark patterns" and include a non-exhaustive list of manipulative design tactics in order to curb abuse and aid enforcement (Page 6);
- Establish a universal opt-out mechanism that makes it easy for individuals to limit the collection, use, and transfer of their data (Page 14);
- Narrowly scope the definition of affirmative, freely given, and specific consent (Page 18);
- Empower individuals to meaningfully exercise their right to opt-out of profiling and automated decision making (Page 25); and
- Define minimum requirements for robust Data Protection Impact Assessments that enable comparative and objective review by both enforcement authorities and consumers (Page 26).

## I. Colorado Privacy Act in the current landscape of privacy regulation

### *How does the CPA compare to other privacy regulation?*

In recent years states have begun to consider legislation broadly regulating the collection and use of personal data online. Nevada passed a privacy law that went into effect in 2019 and was amended in 2021.[4] The California legislature enacted the California Consumer Protection Act ("CCPA") in 2018, which went into effect in 2020. California citizens then approved a ballot initiative to amend CCPA through Proposition 24, or the California Privacy Rights Act ("CPRA"), in 2020. The law, as amended, will go into effect in January of 2023. Colorado passed the Colorado Privacy Act ("CPA") in 2021, which will go into effect in July of 2023. Meanwhile, Virginia passed the Virginia Consumer Data Protection Act ("VDCPA") in 2021, which will also go into effect of January of 2023. In 2022, Utah passed the Utah Consumer Privacy Act ("UCPA"), which will go into effect in December of 2023. In 2022, Connecticut passed the Connecticut Data Privacy Act ("CTDPA"), which will go into effect in July of 2023. And now the United States Congress is considering the American Data Privacy Protection Act ("ADPPA"),[5] which was introduced in the House of Representatives and approved by the Committee on Energy and Commerce by a 53-2 vote.

[4] Nevada Sec. 603A (2018, 2021)
[5] American Data Privacy Protection Act, H.R. 8152 (2022)

The CPA differs in several important ways from existing and prospective privacy legislation: scope, definitions, consumer rights, assessment structure, appeals, and private rights of action.

**Scope.** First, the CPA's scope is narrower in some ways than the CCPA, the CPRA, and Europe's General Data Protection Regulation ("GDPR"). The GDPR, for example, is expansive, including all entities that process personal data as part of their operations in the EU, companies outside of the EU that offer services to those inside of the EU, and companies outside of the EU that monitor the behavior of individuals in the EU.[6] The CCPA and CPRA cover entities processing California residents' personal data which meet the revenue threshold of $25 million, regardless of how much data they process.[7] The current draft CCPA regulations impose significant obligations on "third parties," a term which has a broader scope than "Business" in the CPPA. If enacted, the ADPPA will also likely have a broader scope than the CPA, as it includes entities covered by the Federal Trade Commission ("FTC") Act, common carriers, and many non-profits.[8]

By contrast, the CPA has volume-based thresholds: entities are within the scope of the act only if they process the personal data of 100,000 or more Colorado-based individuals annually or derive revenue or discounts on goods from the sale of the data of over 25,000 Colorado-based individuals.[9] This narrower threshold of inclusion will likely mean that many entities covered under other privacy statutes will not be governed by the CPA.

Conversely, the CPA's scope is likely broader than much of the privacy legislation currently in effect in other states, as its thresholds for inclusion are less restrictive than those in Virginia, Utah, and Connecticut's privacy statutes.[10]

The CPA is unique among state bills in that it does not exempt non-profit organizations. All other state privacy bills exclude non-profit organizations from their scope. Only the ADPPA includes a similarly large set of non-profits within its scope.[11]

**Global opt-out.** No other operative privacy statute in the U.S. requires companies to honor a global-opt out signal, though the California Attorney General indicated that entities

---

[6] Commission Regulation (EU) 2016/679, art. 3, General Data Protection Regulation.
[7] Cal. Civ. Code § 1798.140(c)(1)(A).
[8] American Data Privacy and Protection Act, H.R. 8152, 117th Congress §2(9) (2022).
[9] Colo. Rev. Stat. Ann. § 6-1-1304(b).
[10] The Virginia statute applies to entities that process the data of 100,000 or more people or process the personal data of 25,000 or more people and derive 50% or more of their revenue from the sale of personal data. Va. Code Ann. § 59.1-575. The Utah statute is unique in that it requires both volume and revenue thresholds to be met: covered entities are those that have annual revenues of $25 million or more *and* either (a) process the personal data of 100,000 people *or* (b) derive more than 50% of their gross revenue from the sale of personal data *and* control or process the personal data of over 25,000 individuals. 2022 Utah. Legis. Serv. Ch. 462, SB. 227 §13-61-102(1)(b); Connecticut's statute applies to businesses that (a) process the personal data of 100,000 individuals (excluding data from financial transactions) or (b) process/control the data of 25,000 individuals *and* derive 25% or more of their revenue from the sale of personal data. 2022 Conn. Legis. Serv. P.A. 22-15, §2 (S.B. 6).
[11] H.R. 8152 §2(9)(B).

would be required to adhere to a global opt-out system in its final CCPA regulations, as well as in draft CPRA regulations by the California Privacy Protection Agency.[12] The CPA's explicit inclusion is helpful, as California currently faces challenges due to ambiguous language. If ADPPA is enacted, it would also require all entities to adhere to a "unified opt-out mechanism."[13]

**Controller/processor distinction.** The CPA adopts the controller/processor distinction that was used in the GDPR and mirrored to some extent in nearly all state privacy statutes.[14] The distinction is relevant for determining which responsibilities each entity has under the law.[15] The CCPA does not adopt this distinction but adopts a similar (though not identical) distinction between "businesses," "third parties," and "service providers."[16]

**Definition of "sale."** The term "sale" is used throughout the CPA to prohibit certain behaviors by data controllers or to define the rights that consumers have with respect to their data.[17] The CPA defines "sale" as an exchange for "monetary or other valuable consideration."[18] This definition is in line with that of the CPRA and the Connecticut data privacy laws.[19] However, it is broader than the definition in Utah and Virginia's privacy statutes, which define sale to only include an exchange for monetary consideration.[20]

**Consumer rights.** The CPA articulates similar consumer rights as those found in the GDPR, most state privacy legislation, and the ADPPA—namely: the right to know of and access personal information being collected about oneself, the right to delete such data, the right to correct such data, and the right to export this data in an easily useable format.[21]

However, the privacy laws in some other states limit the exercise of some of these rights to the data provided directly by the consumer, as opposed to all personal data about the consumer.[22] Utah, for example, only gives consumers the right to request deletion of personal data that the consumers themselves provided.[23] In addition, the VDCPA exempts employment and health data from these data subject rights.[24]

---

[12] Cal. Code Regs. tit. 11 § 999.315 (2022).
[13] H.R. 8152 § 210.
[14] Colo. Rev. Stat. Ann. § 6-1-1303(7).
[15] *E.g.,* Colo. Rev. Stat. Ann. § 6-1-1308.
[16] Cal. Civ. Code § 1798.140(c), (v). The CCPA also includes an additional entity category called "third party," distinct from both businesses and service providers.
[17] Colo. Rev. Stat. Ann. § 6-1-1306(1)(a)(I)(B).
[18] Colo. Rev. Stat. Ann. § 6-1-1303(23)(a).
[19] Cal. Civ. Code § 1798.140(t)(1); 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) § 1(26).
[20] 2022 Utah. Legis. Serv. Ch. 462, SB. 227, §13-61-101(31)(a); Va. Code Ann. § 59.1-575.
[21] Colo. Rev. Stat. Ann. § 6-1-1306; Commission Regulation (EU) 2016/679, art. 12-23, General Data Protection Regulation; Cal. Civ. Code § 1798.100; Va. Code Ann. § 59.1-573; 2022 Utah. Legis. Serv. Ch. 462, SB. 227, §13-61-201; 2022 Conn. Legis. Serv. P.A. 22-15, § 4 (S.B. 6).
[22] Va. Code Ann. § 59.1-573-3; 2022 Utah. Legis. Serv. Ch. 462, SB. 227, §13-61-201(2).
[23] 2022 Utah. Legis. Serv. Ch. 462, SB. 227, §13-61-201(2).
[24] Va. Code Ann. § 59.1-572(C)(1),(2).

**Data protection assessments.** The CPA, like the CPRA, the VDCPA, and the CTDPA, require entities to conduct data protection assessments in certain high-risk circumstances.[25] The CPA's requirements for these assessments are substantially similar to those in Virginia and Connecticut: data protection assessments are required when an entity is engaging in (1) targeted advertising, (2) profiling, (3) the sale of personal data, or (4) processing sensitive data.[26] Under the CPA, these assessments are not publicly available, but must be produced for the Department "upon request."[27] This language is slightly less restrictive than the language in the Virginia and Connecticut statutes, which appear to limit disclosures of these assessments to investigations by the Department.[28]

The GDPR and CPRA have similar but not identical provisions. The CPRA requires businesses processing high risk personal information to regularly perform a "risk assessment" about the benefits and drawbacks associated with that processing, per the rules established by the California Attorney General and the CCPA.[29] The GDPR requires an "impact assessment" (a) where there is large scale automated processing, (b) where specific categories of data are being processed, or (c) where publicly available data is being monitored.[30] These requirements make the scope of assessments substantially different than under the CPA.

**Appeals processes.** The CPA requires that covered entities provide an appeals process for instances in which individuals are denied the ability to exercise their consumer rights.[31] The appeals process requirement is similar to other state legislation of this kind (such as those in Virginia and Connecticut).[32] Under Virginia and Connecticut law, controllers must establish an appeals process for consumers who have been denied any of their statutorily-defined rights.[33] Under both statutes, the controller has 60 days to respond to the appeal.[34] However, the UCPA and the CPRA do not provide this sort of appeals process.[35] Under the UCPA, consumers do not have the right to appeal decisions about their requests. Consumers therefore have a wider range of remedies for violations of their rights under the CPA than under the UCPA or the CPRA.

**Private right of action.** Another way that the CPA differs significantly from the CCPA, the CPRA, the GDPR, and (if enacted) the ADPPA is that it does not provide a private right of action.[36] As with the Utah, Connecticut, and Virginia statutes, violations of the statute must be

[25] Colo. Rev. Stat. Ann. § 6-1-1309; CPRA §§ 1798.185(a)(15)(A), (B); Va. Code Ann. § 59.1-576; 2022; 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) § 8.
[26] Colo. Rev. Stat. Ann. § 6-1-1309; Va. Code Ann. § 59.1-576; 2022; 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) §8.
[27] Colo. Rev. Stat. Ann. § 6-1-1309(4).
[28] Va. Code Ann. § 59.1-576(C); 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6),§8(c).
[29] Cal. Civ. Code § 1798.185(a)(15)(B).
[30] Commission Regulation (EU) 2016/679, art. 35, General Data Protection Regulation.
[31] Colo. Rev. Stat. Ann. § 6-1-1306(3)(a).
[32] Va. Code Ann. § 59.1-573(C); 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) §4(d).
[33] Va. Code Ann. § 59.1-573(C); 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) §4(d).
[34] Va. Code Ann. § 59.1-573(C); 2022 Conn. Legis. Serv. P.A. 22-15, (S.B. 6) §4(d).
[35] 2022 Utah. Legis. Serv. Ch. 462, SB. 227; Cal. Civ. Code Title 1.81.5.
[36] Colo. Rev. Stat. Ann. § 6-1-1310(1).

rectified by the Department.[37] This means that consumers have a narrower range of available remedies under the CPA than under the CPRA/CCPA, the GDPR, and ADPPA.

***The CPA's impact and rulemaking going forward***

The passage of the CPA indicates that the people of Colorado are invested in strong privacy protections. The broad scope of the statute, as well as the inclusion of strong mechanisms to empower individuals (such as the universal opt-out mechanism), indicates that Coloradans favor protections that are at the forefront of the movement for stronger privacy laws. The rulemaking by the Department should reflect those values.

Specifically, the Department should adopt rules that encourage clear communication to Colorado residents about their rights under the CPA. Because of the existing state-by-state approach to protecting consumers' privacy, consumers may not understand the ways in which they are protected online or the ways in which Colorado law gives them stronger protection than other states. This, in turn, may lead to these consumers infrequently exercising their rights. The Department should adopt rules that require clear communication to consumers about their rights and available remedies under Colorado law. After the rules are promulgated, the Department should also consider a public education campaign to both inform consumers of their rights under the CPA and inform businesses of their obligations under the law.

## II. The regulations should include clear guidance on what constitutes a dark pattern.

Considering Colorado's goal of promoting consumer rights, EPIC encourages the Department to adopt rules establishing a broad and flexible construction of the definition of dark patterns. Specifically, the Department should establish that platforms may not utilize dark patterns to obtain consent to process data, as required by statute. This rule should apply to circumstances including, but not limited to, when users make an account on a platform, sign up for an online subscription, make an online purchase, select or change privacy settings while using online services, or delete an account or subscription.

***Frameworks and tools exist to help identify dark patterns.***

Colorado should incorporate existing frameworks and taxonomies used to describe, categorize, and identify dark patterns into its rules. Clarifying and adding specificity to the definition of dark patterns will facilitate ease of compliance and enforcement.

Harry Brignull, who coined the term "dark patterns" in 2010, defines dark patterns as "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something."[38] Brignull classified fourteen common types of dark patterns, and his description of each is listed in Table 1 below.[39] Colorado should consider Brignull's

[37] Colo. Rev. Stat. Ann. § 6-1-1311(1)(a).
[38] Harry Brignull, *About This Site*, Deceptive Design, https://www.darkpatterns.org/about-us.
[39] Harry Brignull, *Types of Deceptive Design*, Deceptive Design, https://www.deceptive.design/types.

categorization during its rulemaking because it provides a helpful taxonomy to distinguish dark patterns from persuasive design features that do not manipulate and harm consumers.

| Table 1: Types of Deceptive Design, Excerpted from Harry Brignull's Website "Deceptive Design"[40] | |
|---|---|
| Trick Questions | While filling in a form, you respond to a question that tricks you into giving an answer you didn't intend. When glanced upon quickly, the question appears to ask one thing, but, when read carefully, it asks another thing entirely. |
| Sneak Into Basket | You attempt to purchase something, but somewhere in the purchasing journey the site sneaks an additional item into your basket, often using an opt-out toggle button or checkbox on a prior page. |
| Roach Motel | You get into a situation very easily, but then you find it is hard to get out of it (e.g., a premium subscription). |
| Privacy Zuckering | You are tricked into publicly sharing more information about yourself than you really intended to. Named after Facebook CEO Mark Zuckerberg. |
| Price Comparison Prevention | The retailer makes it hard for you to compare the price of an item with another item, so you cannot make an informed decision. |
| Misdirection | The design purposefully focuses your attention on one thing in order to distract your attention from another. |
| Hidden Costs | You get to the last step of the checkout process, only to discover some unexpected charges have appeared, e.g., delivery charges, tax, etc. |
| Bait and Switch | You set out to do one thing, but a different, undesirable thing happens instead. |
| Confirmshaming | The act of guilting the user into opting into something. The option to decline is worded in such a way as to shame the user into compliance. |
| Disguised Ads | Adverts that are disguised as other kinds of content or navigation, in order to get you to click on them. |

[40] *Id.*

| | |
|---|---|
| Forced Continuity | When your free trial with a service comes to an end and your credit card silently starts getting charged without any warning. In some cases, this is made even worse by making it difficult to cancel the membership. |
| Friend Spam | The product asks for your email or social media permissions under the pretense it will be used for a desirable outcome (e.g., finding friends), but then spams all your contacts in a message that claims to be from you. |

Arunesh Mathur, Jonathan Mayer, and Mihir Kshirsagar also present a robust set of attributes to describe and identify dark patterns.[41] Their taxonomy should be incorporated into Colorado's rulemaking.

First, Mathur, Mayer, and Kshirsagar explain that dark patterns that modify the decision space exhibit the following attributes: asymmetric, restrictive, covert, or disparate treatment.[42] Asymmetric dark patterns impose an outsize burden on users by prominently featuring choices that are beneficial to the platform and obscuring choices that are beneficial to the user.[43] For example, social media platforms often make it difficult for users to switch to more privacy protective settings, making more invasive options that help boost ad revenue the default. Restrictive dark patterns reduce choices available to users.[44]

Mathur, Mayer, and Kshirsagar explain that other dark patterns modify the flow of information and exhibit deceptive or information hiding attributes. Deceptive dark patterns use false statements or omissions to manipulate users' choices.[45] For example, shopping websites often display a timer for a sale (which will not actually expire once the timer runs out) in order to prompt users to make a purchase quickly. Information hiding obscures important information from users. Websites that do not clearly disclose that users are signing up for a subscription service instead of a one-time purchase employ the information hiding dark pattern attribute.[46] Consent interfaces that offer a one-click acceptance but hide more privacy-protective choices behind multiple clicks are another example of information hiding and should be restricted.

Colorado should consider Brignull's categorization and Mayer, Mathur, and Kshirsagar's taxonomy when defining what constitutes a dark pattern and to enhance the specificity and enforceability of the dark patterns provision of the CPA. Consumers have different thresholds for when a design feature would manipulate, subvert, or impair their autonomy, decision-making, or

[41] See, Arunesh Mathur, Jonathan Mayer & Mihir Kshirsagar, *What Makes a Dark Pattern… Dark?: Design Attributes, Normative Considerations, and Measurement Methods,* Chi. Conf. On Hum. Factors In Computing Sys. (May 2021), https://arxiv.org/pdf/2101.04843.pdf.
[42] *Id*.
[43] *Id*. at 7.
[44] *Id*, at 8.
[45] *Id*. at 8.
[46] *Id*.

choice.[47] Colorado's rule should rely on a minimum set of specific, identifiable attributes and categories to define dark patterns that is flexible enough to protect consumers from deceptive action.

Draft regulations by the California Consumer Privacy Agency issued pursuant to the California Consumer Privacy Act set forth principles that businesses must implement for methods of obtaining consent, including:

1. Easy to understand;
2. Symmetry in choice;
3. Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer's choice.
4. Avoid manipulative language or choice architecture. The methods should not use language or wording that guilts or shames the consumer into making a particular choice or bundles consent to subvert the consumer's choice.
5. Easy to execute.[48]

The draft regulations include illustrative examples of each and state that any method that does not comply with the above may be considered a dark pattern. The California regulations provide a strong model for the Department to consult.

***Real examples of dark patterns***

Included below are some examples of dark patterns that harm countless consumers every day. Platforms utilize far more dark patterns than those included in this comment to manipulate consumers into making choices that are counter to the consumers' interest. Colorado should ensure that the CPA covers dark patterns that are currently in use and that the rule can adapt to prevent new uses of dark patterns.

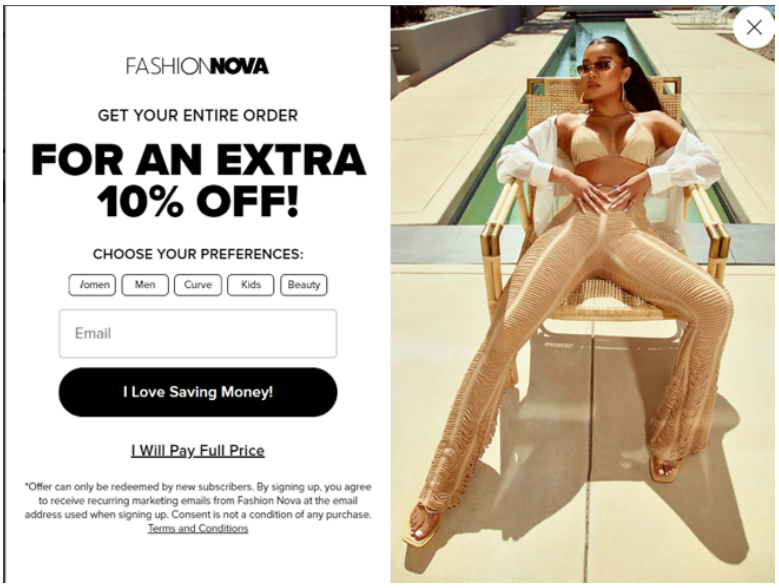
***Consent to purchases***

A 2019 study showed how shopping websites manipulate consumers into making purchasing decisions using dark patterns.[49] The researchers conducted a large-scale analysis of 11,000 shopping websites, finding that 183 websites engaged in 1,818 instances of dark patterns.[50] The shopping websites used a variety of dark patterns to manipulate consumers, including adding additional items to shoppers' carts without consent, signing consumers up for subscriptions without clear consent, displaying a countdown timer for a sale even though the sale would never actually expire, using language to pressure or confuse consumers into making

[47] Colo. Rev. Stat. Ann. § 6-1-1303(9).
[48] Cal. Privacy Protection Agency, Text of Proposed Regulations, Art. 1 § 7004 (2022), https://cppa.ca.gov/meetings/materials/20220608_item3.pdf.
[49] Arunesh Mathur, Gunes Acar, Michael Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Web Transparency (2019), https://webtransparency.cs.princeton.edu/dark-patterns/.
[50] *Id*.

certain purchasing decisions, preselecting more expensive variations of a product, indicating that a product was low in stock or in high demand to encourage consumers to buy quickly even if that was false, and forcing consumers to create an account or share unnecessary personal information to complete their purchase.[51]

For example, Fashion Nova uses a "Confirmshaming" dark pattern in the figure below. The pop-up window uses manipulative language to coerce users into providing their email address to the platform. To accept the 10% offer after entering their email, users must click the button that says, "I Love Saving Money!" If users do not want to enter their email, they must click "I Will Pay Full Price" or the "X" in the corner to close the window.[52] Colorado should clarify that using manipulative language to coerce users into providing information while they are shopping online is prohibited by the CPA.




*Pop-up window on Fashion Nova's website presenting a 10% discount to users who enter their email address. Below the "email" field, a button says, "I love saving money!" Below that button, another button says, "I will pay full price."*

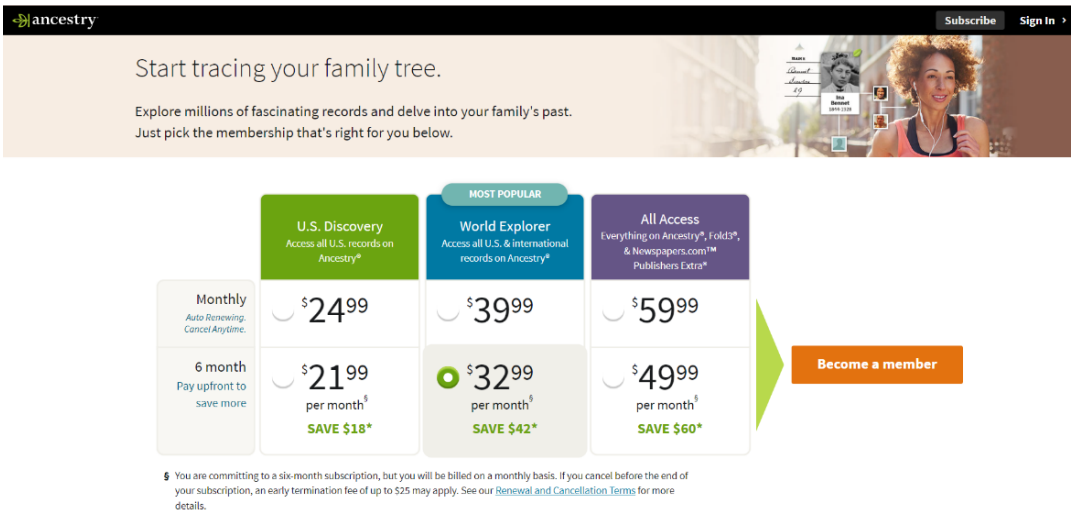
***Consent to subscriptions***

Dark patterns are also prevalent in online subscription models. The FTC issued a settlement order against Age of Learning, Inc., the company that operates the educational children's game ABC Mouse, because the company used dark patterns to manipulate consumers into signing up for subscriptions.[53] FTC Commissioner Rohit Chopra described the dark patterns

[51] *Id.*
[52] Fashion Nova, https://www.fashionnova.com/ (2022).
[53] *FTC Sends Refunds to Consumers Unfairly Billed for ABCmouse Memberships*, Fed. Trade Comm'n (Apr. 19, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/04/ftc-sends-refunds-consumers-unfairly-billed-abcmouse-memberships.

that ABC Mouse used as a "roach motel," using Brignull's category.[54] ABC Mouse did not clearly disclose to consumers that their membership would renew; this information was hidden in the "Terms and Conditions."[55] ABC Mouse is not alone in using dark patterns to manipulate consumers into signing up for a subscription.

In the figure below, Ancestry.com presents an example of a "misdirection" dark pattern. When users choose to create an account, the website presents a variety of price and subscription options to users. The website preselects the option for users to pay for a 6 month "World Explorer" subscription in advance, which is more expensive than other options.[56] Additionally, Ancestry.com's terms state that users' subscriptions will automatically renew unless the user cancels their subscription, even if the user has paid for a certain amount of time in advance.[57] The Colorado rules should protect consumers from the financial harms resulting from similar examples.




*Ancestry.com's subscription page presents 6 different subscription options to users. One option is preselected on the page: a 6 month pre-paid "World Explorer" subscription, which costs $32.99 per month.*

***Deletion***

Platforms also frequently use dark patterns to make it difficult for consumers to delete subscriptions or accounts. The FTC found that ABC Mouse further used dark patterns in making its subscription deletion link difficult to find and the platform often refused to honor customers'

[54] *Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning, Inc.*, Commission File Number 172-3186 (Sept. 2, 2020), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.
[55] *Id.*
[56] *Subscribe*, Ancestry, https://www.ancestry.com/cs/offers/subscribe (last visited Jun. 30, 2022).
[57] *Ancestry Renewal and Cancellation Terms*, Ancestry, https://www.ancestry.com/c/legal/renewal-cancellation-terms (last visited Jun. 30, 2022).

deletion requests.[58] EPIC filed a complaint against Amazon in 2021 for incorporating dark patterns into its subscription model, arguing that their use constituted an unfair and deceptive trade practice.[59] EPIC's complaint built on a report by the Norwegian Consumer Council, which explains that Amazon allows users to sign up for an Amazon Prime subscription in just a few clicks but requires them to navigate an elaborate process to successfully unsubscribe from Prime.[60] Throughout the un-subscribe process, Amazon presents frequent warnings about the benefits consumers will miss out on once they cancel their subscription.[61] If the consumer clicks on any of the warnings throughout the process, the consumer must start the entire process over.[62] EPIC's complaint against Amazon explained that Amazon used a "misdirection" dark pattern in the Amazon Prime cancellation process by changing the text on every stage of the deletion process: "End Membership" changes to "Cancel My Benefits," and then to "Continue to Cancel," and finally to "End Now." Meanwhile, the "Keep My Benefits" button remains the same throughout the deletion process.[63] The figure below shows the different buttons utilized throughout the Amazon Prime deletion process.


*While deleting an Amazon Prime Subscription, users encounter differently worded "Cancel" buttons. The first button says, "End membership," the second says, "Cancel my benefits," the third says, "Continue to cancel," and the last button says "End now."*

[58] *Id*.
[59] Complaint of EPIC, *In re Amazon* (Feb. 23, 2021), https://epic.org/wp-content/uploads/privacy/dccppa/amazon/EPIC-Complaint-In-Re-Amazon.pdf.
[60] Forbrukerrådet, *You Can Log Out, but You Can Never Leave* 27 (Jan. 14, 2021), https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf.
[61] *Id*. at 18.
[62] *Id*.
[63] Complaint of EPIC at 8-9, *In re Amazon* (Feb. 23, 2021), https://epic.org/wp-content/uploads/privacy/dccppa/amazon/EPIC-Complaint-In-Re-Amazon.pdf.

Colorado's rules do not currently prohibit dark patterns used to prevent consumers from deleting their accounts, but these dark patterns pose significant financial and privacy risks to consumers. Colorado should clarify that its rules also prohibit the use of dark patterns to manipulate or coerce users' decisions to revoke consent to process personal data when users choose to delete an account or subscription, as the data is inextricable from maintaining an account.

***Impact of dark patterns on consumers***

Dark patterns harm consumers in three primary ways. First, dark patterns often cause financial harms, for example, by manipulating consumers into unintentionally buying something, signing up for a subscription, or being unable to cancel a subscription. Second, consumers suffer privacy hams when dark patterns manipulate them into sharing private information they did not wish to share. Third, dark patterns impose a significant cognitive burden because consumers must spend excess time, energy, and attention trying to understand an interface or cancel a subscription, to name a few examples.[64]

***Colorado's rules should prohibit dark patterns.***

Given the prevalence of dark patterns online and the pervasive nature of technology in modern society, consumers are likely unable to avoid dark patterns on their own. Colorado should protect its citizens by ensuring that the CPA provides a clear, specific, and holistic definition of dark patterns that encompasses current prevalent types of dark patterns and can adapt to address future uses of dark patterns. Colorado's rulemaking should make clear that platforms may never utilize dark patterns. The rulemaking should ensure that the definition of dark patterns covers manipulative structures related to account and subscription deletion and to making purchase or subscription decisions or select privacy settings.

EPIC recommends the Department incorporate the following language into its regulations:

> "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation."[65]
>
> A Controller shall not employ dark patterns to subvert, impair, or users' autonomy, decision-making, or choices for any reason, including, but not limited to, influencing users' choices to:
>
> - Consent to the processing of personal data

[64] *See*, Arunesh Mathur, Jonathan Mayer & Mihir Kshirsagar, *What Makes a Dark Pattern… Dark?: Design Attributes, Normative Considerations, and Measurement Methods*, Chi. Conf. On Hum. Factors In Computing Sys., May 2021, https://arxiv.org/pdf/2101.04843.pdf.
[65] *See* Cal. Civ. Code § 1798.140(l).

- Delete their account or subscription
- Make purchase or subscription decisions
- Select privacy settings

## III. Establish a universal opt-out mechanism that makes it easy for individuals to limit the collection, use, and transfer of their data

Privacy laws in Colorado, Connecticut, and California all require companies to honor global opt-out requests to some extent,[66] and pending legislation before Congress would do the same.[67] EPIC has recommended that federal and state governments mandate compliance with global opt-out signals, including in comments submitted to the California Privacy Protection Agency,[68] testimony submitted to the Florida House Commerce Committee,[69] a white paper submitted to the FTC,[70] and testimony before the U.S. House Committee on Energy and Commerce.[71] The Department is now requesting input as it drafts regulations detailing "the technical specifications for one or more" global opt-outs as required by the CPA.[72]

***Should the rules point to specific protocols or proposed specifications as exemplars?***

Yes, the Department should point to "Global Privacy Control" (GPC),[73] as an exemplary protocol.[74] For web implementations, the GPC uses an HTTP header to notify every website a user visits that the user does not consent to having their personal information tracked or sold to third parties.[75]

---

[66] Russell Brandom, *Global Privacy Control Wants to Succeed Where Do Not Track Failed*, The Verge (Jan. 28, 2021), https://www.theverge.com/2021/1/28/22252935/global-privacy-control-personal-data-tracking-ccpa-cpra-gdpr-duckduckgo; Interview with Ashkan Soltani (Mar. 12, 2021), https://linc.cnil.fr/fr/ashkan-soltani-enable-users-control-their-privacy-simply-and-effectively-browser.
[67] H.R. 8152 § 210.
[68] Comments of EPIC et al. on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Nov. 8, 2021), https://epic.org/documents/comments-of-epic-and-three-organizations-on-regulations-under-the-california-privacy-rights-act-of-2020.
[69] Letter from EPIC to the Commerce Committee, Florida House of Representatives (Apr. 14, 2021), https://archive.epic.org/state-policy/florida/EPIC-HB969-Apr14.pdf.
[70] Consumer Reports & EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.
[71] *Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing Before the H. Subcomm. on Consumer Protection & Commerce*, 117th Congress (June 14, 2022) (Statement of Caitriona Fitzgerald, Deputy Director, EPIC), https://epic.org/documents/hearing-on-protecting-americas-consumers-bipartisan-legislation-to-strengthen-data-privacy-and-security.
[72] Colorado Department of Law, Pre-Rulemaking Considerations for the Colorado Privacy Act (Apr. 12, 2022), https://coag.gov/app/uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy-Act.pdf.
[73] The standard is available at https://globalprivacycontrol.github.io/gpc-spec.
[74] See more details at Global Privacy Control, https://globalprivacycontrol.org/.
[75] Scott Ikeda, *"Global Privacy Control" Protocol Is the Heir Apparent to "Do Not Track"; Will It Work This Time?*, CPO Magazine (Oct. 14, 2020), https://www.cpomagazine.com/data-privacy/global-privacy-control-protocol-is-the-heir-apparent-to-do-not-track-will-it-work-this-time.

***Should the rules discuss specific considerations tailored for different categories of tools that might serve as global opt-outs, such as browsers, operating system settings, and browser add-ons, or should our rules remain strictly technology neutral?***

Although it is important to establish strong baseline requirements applicable to all global opt-out mechanisms, the Department should not hesitate to address technology-specific considerations where appropriate. For example, while all global opt-out mechanisms must be "consumer-friendly, clearly described, and easy to use by the average consumer,"[76] controllers and consumers may benefit from the inclusion of specific considerations applicable to browser-based opt-out tools and operating-system based opt-out tools. The Department could provide this detail through narrative examples and/or visual depictions of compliant and non-compliant opt-out mechanisms.

***The "rules must adopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the United States." What other similar mechanisms have been required?***

*California Privacy Rights Act (CPRA)*

The CPRA requires every business to "[p]rovide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information" allowing consumers to opt-out of the sale of their personal information.[77] However, businesses are not required to post such a link if they allow consumers to opt out using a global opt-out preference signal.[78] Consumers can override their global opt-out preference on a business-by-business basis, but, as always, they must be able to opt back out as easily as they opted in.[79] Finally, businesses cannot discriminate against consumers who opt out,[80] though businesses may still charge higher prices or provide lower quality if they can demonstrate that the difference is "reasonably related to the value provided to the business by the consumer's data."[81]

In addition, the CPRA requires the California Privacy Protection Agency ("CPPA") to issue regulations defining the "requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information."[82] Moreover, the CCPA requires businesses to treat "user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information" as a request to prohibit the sale of such

[76] Colo. Rev. Stat. Ann. § 6-1-1312(d).
[77] Cal. Civ. Code § 1798.135(a).
[78] *Id.* § 1798.135(b)(1).
[79] *Id.* § 1798.135(b)(2).
[80] *Id.* § 1798.125(a)(1).
[81] *Id.* § 1798.125(a)(2).
[82] *Id.* § 1798.185(a)(19).

information.[83] Currently, businesses must stop selling the consumer's information within fifteen days of receiving the opt-out, and, if any information is sold during that period, the business must direct the information recipient to not sell the information to any other party.[84] Pending regulations implementing the CPRA would require businesses to direct all third parties to stop using the consumer's information, regardless of when they received it.[85] The revisions would also require businesses to offer confirmation that a request has been processed.[86]

*Connecticut Data Privacy Act (CTDPA)*

The CTDPA requires data controllers to honor opt-out preference signals by January 1, 2025.[87] Under the statute, universal opt-out mechanisms must meet the following requirements:

- They cannot unfairly disadvantage another controller.
- They cannot have a default "opt in" or "opt out" setting but must require users to affirmatively opt out.
- They must be "consumer-friendly and easy to use."
- They must be as consistent as possible with other federal or state requirements.
- They must confirm the user's residence in Connecticut and that the opt-out request was legitimate.

If the universal opt-out mechanism conflicts with the user's controller-specific settings or programming, the controller must comply with the universal opt-out request, but the controller can give the user the opportunity to opt in.[88]

The CTDPA provides no rulemaking authority, but it does create a task force to submit findings and recommendations to the General Assembly regarding topics in data privacy, which may include specifications for universal opt-out mechanisms.[89]

***The "rules must permit the controller to accurately authenticate the consumer as a resident of this state." What kind of mechanisms should our rules acknowledge to satisfy this requirement?***

The purpose of the universal opt-out mechanism is to provide a way for individuals to limit the collection of their personal data in a way that is easy for the average consumer, as required per § 6-1-1313(2)(d). So the statute's requirement that a universal opt-out mechanism must permit "authentication" should be interpreted in a way that is consistent with the underlying purpose of the mechanism: to make it easy for the average consumer to opt-out.

---

[83] 11 C.C.R. § 7026(a).
[84] *Id.* § 7026(e).
[85] 11 C.C.R. § 7026(f) (proposed June 8, 2022).
[86] *Id*.
[87] 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) § 6(e)(1)(A)(ii).
[88] *Id.* at § 6(e)(1)(B).
[89] *Id*. at § 12(a)(7).

The simplest way to do this is through a self-certification by the user when the opt-out signal is enabled. However, a more resource-intensive solution would be to permit a controller to independently authenticate the source of an opt-out signal using a commercial geolocation database or IP-to-location service.[90] The statute only requires that a controller be *permitted* to perform an authentication, it does not require controllers to do so and does not require that authentication be enabled by the opt-out mechanism itself. It is important that the implementing regulations do not require controllers to collect additional information from Colorado residents and do not allow controllers to undermine the purpose of the universal opt-out provision, which is to make it easier for consumers to opt-out, or undermine the broader purpose of the statute, which is to protect privacy and prevent manipulative design.

The best implementation of the universal opt-out requirement would limit the amount of information transferred between a consumer and a website or online service to what is strictly necessary to process the request. If the opt-out mechanism includes a signal that the user has self-identified as a resident of Colorado, then that should be sufficient for most controllers. If, however, a controller chooses to use a more resource-intensive authentication process, it should be the controller's responsibility to do so using commercially available tools and the data already provided through the browser or app request (e.g. the Internet Protocol address identified in the HTTP header).[91] This information can be checked against a commercial geolocation database to verify that the signal originated within Colorado, and no further data collection should be necessary.

The Department should not adopt a rule that would permit controllers to implement authentication processes that would undermine a consumers' affirmative and freely-given choice to opt-out through a universal mechanism. We are concerned that some controllers may argue that "authentication" requires them to repeatedly present consumers with notifications or pop-ups asking them to "verify" their choice to opt-out. This would make it harder, not easier, to use a universal opt-out mechanism and would undermine both the purpose of the universal opt-out provision and the dark patterns prohibition in the statute.

## IV. The Department should impose a strict approach to what qualifies as affirmative, freely given, specific, and informed consent.

### *The meaning of "clear, affirmative act" of consent in the context of the bill*

The CPA defines a "clear, affirmative act" of consent as a written statement, including by electronic means, that does not include (1) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing, along with other unrelated information; (2) hovering over, muting, pausing, or closing a given piece of content;

[90] *See generally* Balakrishnan Chandrasekaran et al.., *Alidade: Ip geolocation without active probing. Department of Computer Science*, Duke University Tech. Rep. CS-TR-2015.001 (2015).
[91] *See* Mozilla, *X-Forwarded-For* (2022), https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Forwarded-For.

and (3) agreement obtained through dark patterns.[92] Colorado should further interpret a "clear, affirmative" act of consent to require a meaningful indication of the consumer's wishes.

A narrow reading of an "affirmative act" is consistent with the aims of the CPA: the consumer must be aware of the data being collected from them and actively choose to participate in the collection. Websites often use banners with language such as "by continuing to browse our website, you consent to our use of cookies…," requiring a consumer to visit a different part of the website to view the provider's cookie policy and make any changes to their settings. Cookie banners with no one-click opt-out option do not constitute a meaningful indication of a consumer's intent because they require additional steps that add barriers to the ability of a consumer to protect their own data—an example of "dark patterns."[93] According to a study on dark patterns, removing the "opt out" button from the cookie banner increases consent by 22 or 23 percent, which demonstrates that "consent" given in such circumstances is not indicative of the consumer's true intent.[94] As EPIC has previously noted, "even if consumers had the time to read every privacy policy and statement, they would in most cases come away with woefully incomplete information."[95]

Furthermore, consumers would still not have information on who their data is being sold to; companies often have not yet decided to whom the data will be sold and the purposes for which it will be used at that stage.[96] This lack of information creates a situation where it would be impossible for consent to be fully informed.

These banners may also appear with pre-checked boxes and minimal information, which are inconsistent with an affirmative act on the part of the consumer signifying their intention to share their information.[97] A consumer's active agreement data policies explained in plain language is the only way the definition of "affirmative act" can be met for the purposes of consent in the CPA.

It is not possible to describe every method by which affirmative consent can be granted through a website or an application. But, absent a signal from a user's browser that indicates a

[92] Colo. Rev. Stat. Ann. § 6-1-1303(5)
[93] *Most cookie banners are annoying and deceptive. This is not consent.*, Privacy International (May 21, 2019), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.
[94] Joe Nocera, *How Cookie Banners Backfired,* N.Y. Times (Jan. 29, 2022), https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html.
[95] See EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.
[96] *Id*.
[97] Nicole Olsen, *No Pre-Ticked Checkboxes for Cookie Consent,* Privacy Policies (July 1, 2022), https://www.privacypolicies.com/blog/pre-ticked-checkboxes-cookie-consent/.

preference for not being tracked,[98] there are some key principles that controllers should follow to comply with the CPA:[99]

- Easy to understand
- Symmetry in choice
- Avoid confusing language such as double negatives
- Avoid manipulative language or choice architecture including words that guilt or shame consumers or subvert consumer choice
- Easy to execute[100]

***The meaning of "freely given" or "unambiguous" consent***

Like a "clear, affirmative" act, the bill also requires consent to be "unambiguous" and "freely given."[101] The CPA does not define "unambiguous," but Colorado should interpret this term to mean consent must be explicitly given from a consumer for their data to be processed. The regulations should specify the language controllers may use to obtain consent for data processing so that consumers are giving actual, not implied, consent. Often pop-ups or windows seeking consumer consent allow the consumer to simply exit them and continue using the website as usual, effectively using their silence as implied consent to data collection—arguably constituting a dark pattern that obfuscates the effect of a consumer's action. Since CPA states that agreement gained through dark patterns does not constitute consent,[102] the regulations should make clear that this and other forms of implied consent would not meet the CPA consent standard.[103]

In the absence of browser privacy signals from the consumer, the CPA should be read as requiring the consumer to make an affirmative choice between opting in and opting out before being allowed to use the website or application features.

Other regulatory schemes have yet to define "unambiguous" in the context of consent but provide helpful examples. The EU has ruled that pre-checked boxes violate the requirements for unambiguous consent. Pre-checked boxes offer no evidence that the consumer intentionally consented to the data collection.[104]

---

[98] Colo. Rev. Stat. Ann. § 6-1-1306(1)(a)(II).
[99] For an example, see https://www.cookiebot.com/en/ccpa-compliance/#:~:text=CCPA%20compliance%20with%20Cookiebot%20CMP&text=The%20CCPA%20requires%20that%20businesses,it%2C%20if%20consumers%20request%20it.
[100] 11 C.C.R. § 7004 (proposed June 8, 2022).
[101] Colo. Rev. Stat. Ann. § 6-1-1303(5).
[102] Colo. Rev. Stat. Ann. § 6-1-1303(5)(C).
[103] *See, e.g.*, 11 C.C.R. § 7004 (proposed June 8, 2022),
[104] Aaron Tantleff, et al., *Top European Court Rules Pre-Checked Cookie Consent Boxes Invalid,* The National Law Review (Oct. 11, 2019), https://www.natlawreview.com/article/top-european-court-rules-pre-checked-cookie-consent-boxes-invalid.

The EU's GDPR also provides useful guidelines for what determines "freely given" consent. The law defines the term as "given on a voluntary basis" – the consumer must make a real choice to disclose their data with the collector.[105] Any pressure from the collector or third parties to consent to disclosing sensitive data "renders the consent invalid."[106] Therefore, the Department should stipulate that collectors may not be allowed to materially impair consumers' experience of the website or application based on their decision to opt in or opt out of data collection by including a non-discrimination provision, similar to Connecticut and California. Otherwise, collectors may, in practice, significantly alter the consumer experience and make any subsequent decision to opt into data collection not freely given. This disparate treatment would also affect the GDPR understanding of voluntary and freely-given consent – pressuring consumers to make a specific choice to avoid a bad experience taints consent.

As Colorado develops regulations construing the CPA, we urge the legislature to also consider the impact of leaving the onus of consent to the consumer. Professor Julie Cohen has noted that consent-based approaches to privacy governance are inherently flawed because consumers are unable to understand the nuances of what they are consenting to.[107] Approaching data privacy from the lens of collective governance protects consumers in the long run and holds collectors and third parties to a higher standard of responsibility when it comes to collecting and handling personal information. To that end, the CPA's data minimization provisions must be strictly enforced, and controllers must comply with universal opt-out settings.

***The meaning of "specific" and "informed" consent***

The CPA also requires that consent must be specific and informed. Colorado should clarify that "specific" and "informed" consent means that consumers will have a clear understanding of what data is being collected from them and consent to the purpose for which it will be used. For example, under the GDPR, "specific" consent has been interpreted to mean that consent to a certain use of data will not be bundled with other terms and conditions, and that distinct uses of data require obtaining separate consents.[108] "Informed" consent requires that the consumer must also have a clear understanding of who the entity requesting the information is.[109]

Collectors must also not be able to obtain bundled consent from a consumer for use of an unrelated product, like an email service, and must not be able to process personal data outside the scope of what is reasonable and necessary. To clarify what is reasonable and necessary, Colorado should provide specific use cases. For example, if Business A provides a mobile app designed to create white noise for better sleep, Business A should not collect, or allow another business to collect, consumer geolocation information through its application without the consumer's

[105] Commission Regulation (EU) 206/679, 32, 2016 O.J. (L 119).
[106] *Id*.
[107] Julie Cohen, *How (Not) to Write a Privacy Law,* Knight First Amendment Institute at Columbia University (March 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.
[108] Commission Regulation (EU) 206/679, 32, 2016 O.J. (L 119).
[109] *Id*.

explicit consent because such geolocation information is outside the scope of what is reasonable and necessary in the context of a sleep noises application.

Colorado should interpret these terms narrowly to maximize the data privacy protection afforded to Colorado residents and ensure that controllers and processors are transparent about what information they are processing, storing, and selling. A narrow reading of "specific and informed" consent is consistent with the aims of the CPA: to protect consumers' choice about what information they are disclosing and require companies to be responsible custodians of data.

Colorado must also clarify that consumers are able to revoke consent for the processing of sensitive data or if data is used for purposes incompatible with the original intent of consent. Currently, the law only states that consumers may revoke their consent for the processing of personal data in the context of opt out-signals.[110] Other laws, like the GDPR, specify that consumers must be given the right to revoke consent in any context. The GDPR states:

> [T]he data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.[111]

Connecticut's Data Privacy Act goes further, dictating the timeline by which a data processor must cease to process the data after consumer consent has been revoked.[112] We urge the Attorney General to interpret the CPA to allow consumers to revoke consent at any time, for any reason.

***The meaning of adequate consent from a parent or guardian***

The CPA classifies personal data of children as sensitive, requiring a controller to first obtain consent from the child's parent or lawful guardian before processing. The FTC has laid out guidelines for determining what constitutes consent from a parent or guardian concerning any personal data related to a known child under COPPA standards:

- Signing a consent form and sending it back to the controller via fax, mail, or electronic scan;
- Using a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder;
- Calling a toll-free number staffed by trained personnel;
- Connecting to trained personnel via a video conference;
- Providing a copy of a form of government issued ID that is checked against a database, provided the business deletes the identification from its records when it finishes the verification process; or

[110] Colo. Rev. Stat. Ann. § 6-1-1306(1)(a)(IV)(C)).
[111] Commission Regulation (EU) 206/679, art. 7(3), 2016 O.J. (L 119).
[112] 2022 Conn. Legis. Serv. P.A. 22-15 (S.B. 6) § 6(a)(6).

- Answering a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer[.]

However, parental consent itself is generally inadequate when it comes to data collection from children, and a better practice is to prohibit the practice as a whole and require companies to integrate age-appropriate design into their products. EPIC supports the comments of Common-Sense Media on this topic.

***Limits on requesting updated consumer consent after a consumer has opted out***

Under the CPA, a controller may enable to the consumer to consent through a webpage, application, or similar method to the processing of the consumer's personal data for the purposes of targeted advertising of sale of personal data.[113] This consent would take precedence over the consumer's choice reflected in the universal opt-out mechanism. However, the controller must provide the consumer with "clear and conspicuous" notice about their choices, the categories of personal data the controller wishes to access, why that data is being collected, and how the consumer may withdraw consent. Whatever mechanism is used, the consumer must be able to revoke the consent as easily as it was affirmatively provided. We urge Colorado to require that consumers must be specifically notified the consumer of the conflict with their opt-out preference signal and provide more details on what "clear and conspicuous" is defined as. Controllers may interpret "clear and conspicuous" notice in the form of a cookie or data policy banner on their website or application. The Department should clarify whether such banners are consistent with the language of the CPA.

We are mindful of burdening consumers with privacy choices and consent requests. Colorado instead should enforce strong data transparency obligations for primary use of data; civil rights protections over discriminatory data processing; nondiscrimination rules; data security obligations; and access, portability, correction, and deletion rights. Excessive requests for consent can have a countervailing effect known as consent fatigue, wherein consumers "consent" to various requests to be more efficient without paying attention to what they are consenting to.[114]

***How does the definition of consent in the CPA compare with other passed and proposed legislation?***

The definition of consent in the ADPPA is very strong, and the Attorney General should consider incorporating aspects of the definition into its rules. The definition in ADPPA reads as follows:

> AFFIRMATIVE EXPRESS CONSENT. —
> (A) IN GENERAL. —The term ''affirmative express consent'' means an affirmative act by an individual that clearly communicates the individual's

[113] Colo. Rev. Stat. Ann. 6-1-1306(a)(IV)(C).
[114] *Id*.

freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity that meets the requirements of subparagraph (B).

(B) REQUEST REQUIREMENTS. —The requirements of this subparagraph with respect to a request from a covered entity to an individual are the following:

(i) The request is provided to the individual in a clear and conspicuous standalone disclosure made through the primary medium used to offer the covered entity's product or service, or only if the product or service is not offered in a medium that permits the making of the request under this paragraph, another medium regularly used in conjunction with the covered entity's product or service.

(ii) The request includes a description of the processing purpose for which the individual's consent is sought and—

(I) clearly states the specific categories of covered data that the covered entity shall collect, process, and transfer necessary to effectuate the processing purpose; and

(II) includes a prominent heading and is written in easy-to-understand language that would enable a reasonable individual to identify and understand the processing purpose for which consent is sought and the covered data to be collected, processed, or transferred by the covered entity for such processing purpose.

(iii) The request clearly explains the individual's applicable rights related to consent.

(iv) The request is made in a manner reasonably accessible to and usable by individuals with disabilities.

(v) The request is made available to the individual in each covered language in which the covered entity provides a product or service for which authorization is sought.

(vi) The option to refuse consent shall be at least as prominent as the option to accept, and the option to refuse consent shall take the same number of steps or fewer as the option to accept.

(vii) Processing or transferring any covered data collected pursuant to affirmative express consent for a different processing purpose than that for which affirmative express consent was obtained shall require affirmative express consent for the subsequent processing purpose.

(C) EXPRESS CONSENT REQUIRED. —A covered entity may not infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(D) PRETEXTUAL CONSENT PROHIBITED. —A covered entity may not obtain or attempt to obtain the affirmative express consent of an individual through—

(i) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(ii) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to provide such consent or any covered data.[115]

## V. The Department should require robust disclosure and notice to ensure the right to opt out of profiling is meaningful and enforceable

***Context and concerns***

As computational power increases, companies' and governments' ability to log and analyze data about us increases as well, giving them the ability to facilitate profiling through automated decision making. The practice of profiling may become a black box for consumers and producers alike, where neither is fully aware of the inputs being used or of how their outcomes came to be. Beyond issues of transparency, profiling in and of itself is dangerous and should be strictly limited and regulated.

Profiling implicates civil rights when used to make decisions in areas like housing, employment, and criminal justice, especially when factors such as race and socioeconomic status are used as inputs. Proxies for this information are also commonly used and must be regulated similarly. Demographic markers such as race and gender are considered sensitive under § 6-1-1303(24), which means consumer consent is required for processing under § 6-1-1308(7). But given the risk of inaccurate and unjust outcomes from profiling, especially when used on people of color,[116] it is vital to guard against the possibility of discriminatory impact. To take one example: for every 100 similar applicants seeking mortgage loans in Denver, Aurora, and Lakewood, only 4 white applicants are denied loans, while 6 Black, Latino, and Asian/Pacific Islander applicants receive denials.[117]

---

[115] H.R. 8152 §2(1).

[116] *See, e.g.*, James Vincent, *Google 'fixed' its racist algorithm by removing gorillas from its image-labeling tech*, The Verge (Jan. 12, 2018), https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai (reporting that Google fixed Google Images' mis-categorization of black people as gorillas by removing the service's ability to identify gorillas outright); Kathleen McGrory and Neil Bedi, *Targeted*, Tampa Bay Times (Sept. 3, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/ (reporting that the Pasco County Sheriff Office created a profiling system to classify those it thinks are likely to break the law so the police may then "make their lives miserable until they move or sue"); Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms (reporting that mortgage loan applicants of color were 40%–80% more likely to be denied than their White counterparts, and that the disparity was over 250% in certain metro areas, even when accounting for factors such as income).

[117] *Id*.

Moreover, profiling is often used as a pretense for further indiscriminate data collection. Profiles made by one firm may be used and processed by others, increasing the amount of data and power companies and governments have over individuals.

***Recommendations***

The Colorado Privacy Act's right to opt out of profiling is a major stride for privacy and civil rights, but it is crucial to bolster that right with transparency concerning when and how profiling occurs. Empowering consumers means making them aware that profiling systems are being used in the first place and providing sufficient detail to allow an individual to opt out.[118] It is crucial that individuals have access not only to user-friendly opt-out methods but also a plain-language explanation of the inputs, programming logic, and purpose of any given profiling process.[119] At a minimum, we urge that a business be required to disclose the purpose of each automated decision-making system it uses to make or assist in determinations about individuals; how the system is being used; the factors the system relies on; a plain-language explanation of the logic of the system;[120] the sources and life cycle of the data processed by the system, including any brokers or other third-party sources involved in the data life cycle; and how the system has been evaluated for accuracy and fairness, including links to any audits, validation studies, or impact assessments. This key information can be provided to individuals through data protection impact assessments.

Widely supported AI principles including the Universal Guidelines for Artificial Intelligence underscore the need for transparency and human control[121] and should inform the Department's rulemaking. The decision of whether to opt out under § 6-1-1306(1)(a)(I)(c) should be an informed one. Accordingly, the Department should interpret (a)(III)'s requirement to provide a "clear and conspicuous" method to opt out as requiring the disclosure of accurate information about the use and construction of profiling systems.

The CPA forbids processing "processing personal data...for profiling if the profiling presents a reasonably foreseeable risk of (I) unfair or deceptive treatment of, or unlawful disparate impact on consumers." Prohibiting disparate impact on consumers is a powerful tool to protect against discriminatory outcomes. Impact is the correct lens for such harm analysis because it focuses on how profiling technology is used and misused.

---

[118] Comments of EPIC et al. on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Nov. 8, 2021), https://epic.org/documents/comments-of-epic-and-three-organizations-on-regulations-under-the-california-privacy-rights-act-of-2020.

[119] *Id.*

[120] For example, in a predictive profiling system or automated decision-making system, the explanation should include data sources and how particular inputs affect determinations (e.g., if a criminal arrest in the last three years increases a "risk" classification by two points).

[121] The Public Voice, *Universal Guidelines for Artificial Intelligence* (2018), https://thepublicvoice.org/ai-universal-guidelines/.

## VI. The Department should set minimum requirements for data protection impact assessments to ensure consistent accountability.

Data protection impact assessments under the CPA must be both meaningful and logistically feasible. The Department must decide (1) what information comprises an assessment; (2) the process of how companies should report this information and ensure its availability to consumers; (3) whether the developer of a system and/or the user of that system should be responsible for completion of assessments; (4) how to make this information public; and (5) methods for review or enforcement and consequences for insufficient or misleading information.

We urge the agency to mandate, at minimum, that a business disclose the purpose of an automated decision-making system; how the system is being used; the factors the system relies on; a plain-language explanation of the logic of the system; the sources and life cycle of the data processed by the system, including any brokers or other third-party sources involved in the data life cycle; and how the system has been evaluated for accuracy and fairness, including links to any audits, validation studies, or impact assessments.

The E-Government Act of 2002 offers a useful starting point for scoping the data protection aspects of the impact assessment. Before initiating a new collection of personal information or procuring information technology that will process personal information, a federal agency must conduct, review, and publish a privacy impact assessment that explains:

(I) what information is to be collected;
(II) why the information is being collected;
(III) the intended use of the agency of the information;
(IV) with whom the information will be shared;
(V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and]
(VI) how the information will be secured.[122]

Additionally, an impact assessment must measure *impact* and not just design choices. In a growing number of countries, users of automated decision-making systems are required to undergo algorithmic impact assessments prior to use or continued use. In Canada, for example, businesses input information about automated decision-making systems into a standardized survey, which allows for the evaluation of system based on design attributes, the sensitivity of data processed, and the system's connection to areas requiring additional considerations and protections.[123] This type of form is something the Department could use to collect and ensure uniform reporting of key information about automated decision-making systems. The Canadian assessment asks each business to evaluate the stakes of the decisions that a system makes, the

[122] E-Government Act, Pub. L. No. 107-347, §§ 208(b)(2)(B)(ii), 116 Stat. 2899, 2922 (Dec. 17, 2002) (codified at 44 U.S.C. § 3501 note).
[123] Canada Digit. Servs., *Algorithmic Impact Assessment* (2021) https://open.canada.ca/aia-eia-js/?lang=en.

vulnerability of subjects, and whether the system is a predictive tool.[124] The tool also allows for multiple answer options and detailed explanations of responses. In some cases, the Canadian tool requires a business to identify the downstream processes of a system. This includes asking (1) whether the system will only be used to assist a decision-maker; (2) whether the system will be making a decision that would otherwise be made by a human; (3) whether the system will be replacing human judgment; (4) whether the system will be used by the same entity that developed it; and (5) for details about the system's economic and environmental impacts.[125] The Department should consider requiring similar reporting from businesses that deploy or sell automated decision-making systems.

We also recommend using the ten "constitutive components" of a strong Algorithmic Impact Assessment as articulated by scholars from Data & Society:

- Signing a consent form and sending it back to the controller via fax, mail, or electronic scan;
- Sources of Legitimacy
- Actors and Forum
- Catalyzing Event
- Time Frame
- Public Access
- Public Consultation
- Method
- Assessors
- Impacts
- Harms and Redress[126]

EPIC recognizes the Department may be unable to review every assessment in detail. For this reason, it is important that the Department require at least one version of each impact assessment to be made public, subject only to the narrow redactions necessary to protect data security and trade secrets. The Department should also require the inclusion of certain data points that can be compared and aggregated across all DPIAs—for example, whether systems process certain types of personal data or are used in certain contexts. The Department should prioritize systems that conduct high-risk processing, and establish criteria that they can use to evaluate many DPIAs efficiently, but allow the Department to change these predefined elements over time based on enforcement experience.

[124] *Id.*
[125] *Id.*
[126] Emmanuel Moss et al., *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest*, Data & Society (June 21, 2022) https://datasociety.net/wp-content/uploads/2021/06/Assembling-Accountability.pdf.

We urge the agency to establish clear minimum baselines and methods of disclosure to secure meaningful information for Colorado residents about each automated decision-making and profiling system.

## VII. Conclusion

EPIC applauds the Department's open and robust process to promulgate rules to protect consumers in accordance with the Colorado Privacy Act. EPIC will continue to be available for future discussion about our recommendations about how the Department can best protect Coloradans as per the CPA.

Sincerely,

Alan Butler, EPIC Executive Director
Caitriona Fitzgerald, EPIC Deputy Director
John Davisson, EPIC Senior Counsel
Ben Winters, EPIC Counsel
Calli Schroeder, EPIC Global Privacy Counsel
Sarah Al-Shalash, EPIC IPIOP Clerk 2022
Caroline Kraczon, EPIC IPIOP Clerk 2022
Paul Meosky, EPIC IPIOP Clerk 2022
Hansy Piou, EPIC IPIOP Clerk 2022
Divya Vijay, EPIC IPIOP Clerk 2022