Comments of the Electronic Privacy Information Center,
Consumer Federation of America, and Fairplay

to the

COLORADO DEPARTMENT OF LAW
On Pre-Rulemaking Considerations for the Automated Decision-Making Technology (S.B. 26-189) and Chatbot Safety (H.B. 26-1263) Acts

July 13, 2026

The Electronic Privacy Information Center ("EPIC"), Consumer Federation of America ("CFA"), and Fairplay submit these comments in response to the invitation of the Colorado Department of Law for input from stakeholders prior to the proposed rulemaking required by S.B. 26-189: Automated Decision-Making Technology ("ADMT") in Consequential Decisions and potential rulemaking on H.B. 26-1263: Chatbot Safety Act. EPIC welcomes the opportunity to comment on the questions posed prior to these rulemakings and applauds the Department's use of its authority to promulgate rules that help support the protection of consumers.

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] CFA is an association of non-profit consumer organizations based in Washington, D.C. that was established in 1968 to advance the consumer interest.[2] Founded 25 years ago, Fairplay is a national, independent nonprofit organization dedicated to protecting children from unfair commercial practices in media and digital environments, where it is a nationally recognized expert.[3]

EPIC has a long history of advocating for safeguards for businesses' use of ADMTs, including engaging in similar rulemaking processes in other states.[4] CFA has long advocated at both state and federal levels for commonsense regulations on automated decision-making tools

---

[1] EPIC, *About EPIC* (2026), https://epic.org/about/.
[2] CFA, *About CFA* (2026), https://consumerfed.org/about-cfa/.
[3] Fairplay, *About* (2026), https://fairplayforkids.org/mission-impact/.
[4] EPIC, Comments to the CPPA on Proposed Regulations Regarding Cybersecurity, Risk Assessments, and ADMTs (Feb. 19, 2025), https://epic.org/documents/comments-to-the-cppa-on-proposed-regulations-regarding-cybersecurity-risk-assessments-and-admts/.

that impact investor protections, junk fees, job opportunity, housing opportunities, and more, urging transparency, bright-line rules, and meaningful accountability.[5]

EPIC, CFA, and Fairplay have also been heavily involved in shaping chatbot policy at both the state and federal level, including developing a model chatbot bill that has been considered by seven states so far in 2026 and was recently introduced in Congress.[6]

For years, EPIC has advocated for language that strengthens Colorado residents' ability to exercise their rights and prevents algorithmic discrimination and risks to privacy, including throughout the years of legislative debate leading up to the adoption of S.B. 26-189 and during the enactment and rulemaking on the Colorado Privacy Act.[7] Both Colorado's Privacy Act and Consumer Protection Act have paved the way in increasing corporate accountability and transparency to benefit consumers. ADMTs introduce a new vector of risk for everyday Coloradans that often occurs behind the shadow of the corporate "black box." With strong, consumer-minded rulemaking, the Department can better protect consumers by closing some of the corporate-friendly loopholes the existing language in S.B. 26-189 may create.

In addition to the existing Colorado laws[8] that developers and deployers of ADMTs are still, of course, subject to, EPIC, CFA, and Fairplay encourage the Department to consider the following as the rulemaking process commences.

---

[5] *See, e.g., CFA Letter to CFPB on the need for 'Less Discriminatory Algorithms,'* CFA (June 2024), https://consumerfed.org/news/testimony-comments/urgent-call-to-cfpb-for-regulatory-clarity-on-the-need-to-search-for-and-implement-less-discriminatory-algorithms/; *CFA Testimony in Support of the New York AI Act*, CFA (Jan. 2026), https://www.nysenate.gov/sites/default/files/admin/structure/media/manage/filefile/a/2026-01/ben-winters-consumer-federation-of-america-testimony.pdf.

[6] EPIC, *EPIC Applauds Introduction of Privacy-Centered Federal Chatbot Bill* (July 10, 2026), https://epic.org/press-release-epic-applauds-introduction-of-privacy-centered-federal-chatbot-bill-2/; People-First Chatbot Act, 119th Cong. (2d Sess. 2026), https://foushee.house.gov/imo/media/doc/final_people-first_chatbot_act.pdf.

[7] EPIC, *Building on Colorado's AI Act to Ensure Sound Policy*, https://epic.org/documents/building-on-colorados-ai-act-to-ensure-sound-policy/.

[8] *See, e.g.,* Colo. Rev. Stat. §§ 6-1-101 to -116, -1301 to -1314, 24-34-601 to -605 (2026); 42 U.S.C. §§ 2000e to 2000e-17 (2026).

I. Responses to Targeted Questions for Informal Input on the ADMT Act (Section IV)

1. Definitions of Materially Influence & Other Terms

a. How could regulations clarify current definitions of "ADMT," "materially influence," or "consequential decision"? How can they provide guidance to ensure that these definitions are not interpreted too broadly or too narrowly? What are the concerns if the definition is interpreted too broadly or too narrowly?

EPIC, CFA, and Fairplay support the definitions of "ADMT" and "materially influence" that have been adopted by S.B. 26-189 but urges the Department to broadly construe the definition of "consequential decision." As it stands, the current definition risks being interpreted too narrowly such that it could exclude some important decisions and use cases of ADMTs and potentially leave consumers vulnerable. Further, overly narrow language can create corporate loopholes that similarly pose unintended consequences and risks to consumers.

In line with the definition of "ADMT," the definition of "consequential decision" should include cases where ADMTs are used to "make, guide, or assist a decision, judgment, or determination concerning an individual," and should therefore be broadened to adequately do so and avoid conflicting interpretations. This definition could be broadened to include coverage of:

- Uses of ADMT that have the potential to meaningfully impact any person's safety or well-being, including mental, emotional, and reputational well-being;
- Uses of ADMT in which the outputs facilitate decisions with legal or similarly significant effects on any person's civil rights, civil liberties, privacy, or equal opportunities; and
- Uses of ADMT in which the outputs can impact any person's access to or significant change in the price of critical benefits, resources, or services.[9]

Examples of the above ADMT uses could be useful in broadening the meaning of what constitutes a "consequential decision" and could help counteract the narrowing effect that the list of exemptions in § 6-1-1701(3)(b) could lead to. In listing examples, the Department should be clear that any listed examples of consequential decisions are not comprehensive to ensure long-term flexibility as technology continues to evolve. Further, these examples should make clear that even when humans are involved in the decision-making, decisions where the use of ADMTs

---

[9] Kara Williams, *AI Legislation Scorecard: A Rubric for Evaluating AI Bills*, EPIC (June 2024), https://epic.org/wp-content/uploads/2024/06/EPIC-AI-Legislation-Scorecard-June2024.pdf.

nonetheless guides or assists in the decision-making process can still be subject to this law; simply having a human act as a final "rubber stamp" on a decision does not suffice for exemption. The ACLU's comments outline many other potential use cases that EPIC, CFA, and Fairplay also support including.[10] Below are a few examples of different "consequential decisions" that could be listed to expand the scope of protection of this law:

- Students' placement into advanced courses or gifted programs
- Special education eligibility and placement
- Eligibility or removal from extracurricular activities
- Academic tracking decisions
- Awards or denial of certificates or credentials
- Eligibility for advancement tracks or leadership pipelines in an employment context
- Layoff selection or ranking in workforce reduction
- Eligibility for remote work or hybrid status
- Unit assignment within a property (size, location, quality) when renting or purchasing home
- Driver risk scoring in auto insurance
- Coverage applicability determinations in insurance
- Limits on frequency, duration, or intensity of medical care
- Determinations about eligibility and access to essential government services and public benefits
- Electronic monitoring assignment decisions

While some of the exceptions listed in § 6-1-1701(3)(b) are useful and will appropriately exclude tools unlikely to cause harm like spellcheck and spam-call filtering, we recommend adding some clarifications to avoid misinterpretation. For example, with regards to the exception in § 6-1-1701(3)(b)(IV), the Department should clarify that using an AI system that doesn't typically generate a score or prediction, like ChatGPT, does not exempt an entity from complying with the law. While using ChatGPT or another summarization tool in a decision-making process doesn't automatically subject an entity to this law, if ChatGPT is used to generate a score or prediction that is used in a decision-making process, then its use should fall under this law's coverage. The Department should also clarify the intent of the exception in § 6-

[10] ACLU, Pre-Rulemaking Comment to the Colorado Attorney General's Office on Automated Decision-Making Technology Act and Chatbot Safety Act, (submitted July 6, 2026), https://coag.my.salesforce.com/sfc/p/#t00000004XX8/a/cs00000vnDg1/FJGIujZz1IXvxDWjRHpU8glaQmYwjJ5SxkfHhUG3kcc.

1-1701(3)(b)(IX), given the examples that would be included in an educational setting above, and ensure that this exemption is narrowly interpreted.

b. Are there frameworks or other laws that the Department can look to in drafting regulations related to the definitions of these terms?

As the Department begins the rulemaking process, EPIC, CFA, and Fairplay recommend that the Department refer to the following laws and resources to enhance and strengthen its definition of "consequential decision" and other areas of the law as described in this comment:

- Regulations enacted by the California Privacy Protection Agency covering ADMTs[11]
- EPIC's AI Legislation Scorecard[12]
- EPIC's prior testimony calling for the strengthening of the Colorado AI Act[13]
- Consumer Reports' AI Policy Recommendations[14]
- Colorado Privacy Act Rules[15]
- EPIC's prior advocacy during the Privacy Act rulemaking process in 2023[16]

c. How can the rulemaking process help to ensure the Act interoperates with existing federal and state laws related to ADM, discrimination, privacy, and consumer protection?

Though this Act applies specifically to ADMTs, developers and deployers alike are nevertheless still required to comply with all other federal and Colorado state laws. The Department should enact rules that refer to existing Colorado laws that similarly aim to protect consumers, such as the Consumer Protection Act,[17] the Colorado Privacy Act,[18] the Colorado Anti-Discrimination Act,[19] and other sectoral laws prohibiting discrimination in employment,

---

[11] Cal. Code Regs. tit. 11, §§ 7200–7222 (2026), https://cppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf.
[12] Williams, *supra* note 895.
[13] EPIC, *supra* note 67.
[14] Grace Gedye, *CR Publishes Artificial Intelligence Policy Recommendations*, Consumer Reports (Mar. 5, 2024), https://innovation.consumerreports.org/cr-publishes-artificial-intelligence-policy-recommendations/.
[15] Colorado Privacy Act Rules, 4 Colo. Code Reg. § 904-3 et seq., https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf.
[16] EPIC, *Colorado Privacy Act Revision Comments* (Jan. 12, 2023), https://epic.org/documents/colorado-privacy-act-revision-comments/.
[17] Colo. Rev. Stat. §§ 6-1-101 to -116.
[18] *Id.* §§ 6-1-1301 to -1314.
[19] *Id.* §§ 24-34-601 to -605.

housing, insurance, and other areas.[20] Similarly, the Department should draft rules that align with federal anti-discrimination laws like Title VII of the Civil Rights Act.[21]

2. Post-adverse outcome disclosure requirements

a. Is the definition of "adverse outcome" sufficiently clear or is additional guidance necessary?

EPIC, CFA, and Fairplay strongly urge the Department to promulgate rules that clarify what constitutes the important threshold of an "adverse outcome" such that consumers are sufficiently able to exercise the rights that have been granted to them within § 6-1-1704(3). As it stands, this definition risks being narrowly construed to a binary, where consumers who seemingly receive a "positive outcome" could nevertheless have been adversely affected by the use of ADMT. For example, even if the use of an ADMT leads to an otherwise equal alternative option than an entirely human-made decision would result in, there is a degree of self-determination lost in favor of algorithmic pre-determination that impedes personal rights to autonomy. Expanding the definition to include results that result in "materially less favorable differentiated price, cost, compensation, or other material terms" is helpful in expanding this definition yet still leaves users at risk of being unable to exercise their rights if interpreted too narrowly.

A broader, clarified definition of "adverse outcome" should be based on what is perceived by the affected consumers as adverse, not what deployers deem to be an adverse decision. As this law is meant to protect consumers from harm and hidden ADMT use, allowing deployers to decide what an "adverse outcome" is would only frustrate this purpose and create possibility for loopholes. Therefore, EPIC, CFA, and Fairplay urge the Department add language to avoid this pitfall.

---

[20] *See generally id.* §§ 24-34-101 to -1008.
[21] 42 U.S.C. §§ 2000e to 2000e-17

b. How can rulemaking provide standards that help to ensure the disclosures of information are sufficiently accurate, detailed, and informative while remaining reasonably understandable to consumers and not overly onerous for deployers?

As described throughout this comment, it is imperative that disclosures are written in plain language and are specific enough for individuals to identify whether the decision made about them was based on inaccurate or incomplete information. Without such disclosures, the burden weighs disproportionately heavy on consumers to prove not only that they were subject to an ADMT, but how it affected their decision. If a consumer believes they are discriminated against or their civil rights pursuant to another state or federal law have been violated, pursuing a claim will require such information to be available.

Despite anticipating that businesses may argue that these disclosures are overly burdensome, this law's purpose and intent is to protect consumers from obscure and discriminatory ADMTs, not to make using them easier on businesses. This law has already been amended significantly to ease burdens on businesses; the remaining consumer rights, especially their access to information about how life-altering decisions about there are being made, must be broadly construed to truly protect consumers, and fulfill the legislative intent behind this law.

c. How specific should the guidance be to clarify the content of required disclosures related to categories, sources, or types of personal data that must be disclosed following an adverse decision?

The Department should provide specific guidance to businesses requiring disclosures to include what information and types of data were used to make consequential decisions to ensure that consumers see the whole picture. It will be impossible for consumers to know whether to exercise their right to correct inaccurate personal data, for example, if they are not given access to the specific personal data that was used to make the decision about them. Similarly, an overly vague disclosure can be just as useless to a consumer as no disclosure at all if it does not provide them with actionable details with which to challenge an adverse decision. Therefore, the Department should be as prescriptive as possible in describing what categories and level of detail of information businesses must provide to consumers following an adverse decision.

d. **What guidance might be useful to address how the disclosure requirements interact with federal or state laws?**

As above, remembering that developers and deployers are still subject to existing federal and state law, the Department should enact rules that refer to existing Colorado laws that similarly aim to protect consumers, such as the Consumer Protection Act,[22] the Colorado Privacy Act,[23] the Colorado Anti-Discrimination Act,[24] and other sectoral laws prohibiting discrimination in employment, housing, insurance, and other areas.[25] Similarly, the Department should draft rules that align with federal anti-discrimination laws like Title VII of the Civil Rights Act.[26]

e. **Are there standards under other regulations or laws that should be used to guide regulations concerning how to describe the role of a covered ADMT in a consequential decision to consumers?**

As above, EPIC, CFA, and Fairplay recommend the Department refer to the following laws and resources to enhance the disclosures required when ADMTs are used in consequential decisions:

- Regulations enacted by the California Privacy Protection Agency covering ADMTs[27]
- EPIC's AI Legislation Scorecard[28]
- EPIC's prior testimony calling for the strengthening of the Colorado AI Act[29]
- Consumer Reports' AI Policy Recommendations[30]
- Colorado Privacy Act Rules[31]
- EPIC's prior advocacy during the Privacy Act rulemaking process in 2023[32]

---

[22] Colo. Rev. Stat. §§ 6-1-101 to -116.
[23] *Id.* §§ 6-1-1301 to -1314.
[24] *Id.* §§ 24-34-601 to -605.
[25] *See generally id.* §§ 24-34-101 to -1008.
[26] 42 U.S.C. §§ 2000e to 2000e-17
[27] Cal. Code Regs. tit. 11, §§ 7200–7222 (2026), https://cppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf.
[28] Williams, *supra* note 9.
[29] EPIC, *supra* note 7.
[30] Gedye, *supra* note 14.
[31] 4 Colo. Code Reg. § 904-3.
[32] EPIC, *supra* note 16.

3. Consumer notice requirements prior to the use of covered ADMTs

a. Should further guidance or examples be provided to clarify what constitutes as "clear and conspicuous" notice to consumers?

To ensure that consumers are adequately informed that ADMT is being used and, thus, able to exercise their rights within this statute should they choose to do so, it is critical that deployers provide clear, conspicuous, and understandable notice. EPIC, CFA, and Fairplay urge the Department to adopt rules that clarify the manner by which deployers must provide "clear and conspicuous" notice to consumers. Specifically, the following requirements should be included to clarify the scope of the required notice:

- Plain, straightforward description of the ADMT system and its purpose that is readily understandable to a reasonable person and avoids overly technical or legal jargon;
- The nature of the output decision;
- The personal information the system assesses and how it was assessed;
- The relevance of and weight given to different personal characteristics and information to the final decision;
- Any human components of the system;
- Contact information for the deployer;
- Details about the data on which the ADMT system was trained;
- Procedures for ongoing testing and evaluation of the ADMT to ensure it is working as intended; and
- Whether the ADMT used in the decision underwent the impact assessment required by the Colorado Privacy Act's profiling provisions and, if so, a description of how the business weighed the risks, benefits, and mitigations of risks as required by the law.

Since Coloradans have the right to opt out of the processing of their personal data and both controllers and processors are required to abide by this request, along with universal opt-out requests, deployers should display a notice to inform Colorado citizens of their rights.[33] If a consumer chooses to opt out of data processing, deployers should provide notice to consumers about the manner in which their decision will be made alternatively. When deployers make

[33] *See* Colo. Rev. Stat. § 6-1-1306(a).

changes to their systems in a manner that affects consumers, deployers should also be required to notify consumers in a similar manner of these changes.

b. What form of notice is most useful to consumers to inform them ADMT is being used?

Clear and timely notice to consumers is crucial to allow them to exercise their rights should they choose to do so. EPIC, CFA, and Fairplay urge the Department to adopt rules that clarify the manner through which notice should be provided to consumers and recommend including the following:

- Notice must be presented prominently and conspicuously to the consumer at or before the point when the deployer collects the consumer's personal information that the deployer plans to process using ADMTs.
- Notice must be presented in a conspicuous manner consistent with how the deployer generally interacts with the consumer.
- Notice should be available in a format that makes the disclosure readable to all potential devices, including both on desktop web pages and on smaller, mobile screens.
- Notice should be in languages in which the deployer generally, in its ordinary course of business, would provide contracts and disclaimers, for example, to consumers within the state of Colorado and should be available to the consumer in the language in which service is being offered.
- Disclosures should be reasonably accessible to consumers with disabilities in line with the generally recognized industry standards and applicable state and federal law.

As deployers are also required to comply with the Colorado Consumer Protection Act and Consumer Privacy Act, EPIC, CFA, and Fairplay advise the Department to consider both laws in their rulemaking process. Deployers are prohibited from retaliating against consumers for exercising their rights—including the right to opt out of both the sale of their personal data and its processing to profile and influence decisions about them. Developers and deployers are also both required to comply with universal opt-out requests.

The use of dark patterns or other manipulative design to subvert individuals' decision-making, including in their provision or withdrawal of consent to allow the processing of their personal information, is also explicitly regarded as a deceptive act under § 6-1-105(1)(nnn) that the Department has the authority to enforce as well as in the Colorado Privacy Act.[34] Similarly, the use of dark patterns or a deceptive design to mislead consumers about the use of ADMT should be prohibited.

EPIC, CFA, and Fairplay also urge the Department to revisit § 6-1-1704(2) allowing for a prominent, public notice to be sufficiently compliant, and recommends clarifying that this notice must meet the above requirements of both substance and format. For example, California's CCPA regulations addressed what they refer to as "consolidated pre-use notice," but they clarify both when this type of notice may be used, and that it is subject to the same requirements as any other pre-use notice.[35]

4. Additional Recommendations

Additionally, EPIC, CFA and Fairplay recommend the Department utilize this rulemaking opportunity to strengthen this law and the protections for consumers in several key ways.

a. Require risk assessments.

EPIC has long advocated for a risk assessment to be required prior to deploying an ADMT. The Colorado Privacy Act, for example, requires controllers to conduct data protection assessment prior to processing personal data that the Department has the right to request access to.[36] Going further, California's CCPA regulations enacted by the CPPA require risk assessments when businesses use ADMTs for significant decisions concerning a consumer, when automated processing is used to infer a characteristic about a consumer, and when personal information about consumers is processed to train an ADMT.[37] These regulations also list examples to illustrate when businesses must conduct risk assessments.

---

[34] § 6-1-105(1)(nnn). *See also* § 6-1-1303(5)(b)(c).
[35] *See* Cal. Code Reg. tit. 11, § 7220(e)
[36] Colo. Rev. Stat. § 6-1-1309.
[37] Cal. Code Reg. tit. 11, §§ 7150–7157.

EPIC published a report that explains in further detail why risk assessments are critical to increasing transparency and accountability and has included a list of components to develop an ideal risk assessment framework.[38]

EPIC, CFA, and Fairplay urge the Department to take this rulemaking opportunity to clarify that risk assessments should be conducted prior to the deployment of ADMTs to avoid unnecessary harm for consumers and remain consistent with the Colorado Privacy Act.

b. Avoid sector-specific guidance that lowers the bar for some companies and leaves consumers at risk.

While sector-specific add-ons and guidance can be helpful where appropriate, EPIC, CFA, and Fairplay encourage the Department to set a high bar for all companies regardless of sector. ADMTs carry a similar set of risks to consumers regardless of which industry they are used in. The Department should avoid modifying this law through rulemaking in a way that could incidentally create more loopholes and confusion for businesses than necessary.

c. Clarify the limited scope of developers' and deployers' "right to cure" violations of law.

The Department should take this rulemaking opportunity to clarify the limited scope of the "right to cure" currently provided by § 6-1-1706 to avoid potential loopholes. The provision gives the Department discretion to determine if a cure is possible and, if so, allow the developer or deployer 60 days to cure upon notice of a violation of the law, unless they find that the company knowingly or repeatedly violated the law. The Department should clarify that there will be few occasions in which a cure may be "deemed possible." In many of the decisions covered under the law, an adequate cure is *not* in fact possible; based on the ADMT output a consumer receives, several other decisions and actions may have already had a domino effect stemming from this result within that sixty-day timeframe, and a consumer would have no recourse at all. For example, if a business denies a consumer a job, apartment, or mortgage based on the use of an ADMT, there is no cure for that adverse decision—the job or apartment has likely already been given to someone else, and the house the consumer was hoping to finance is likely already

[38] Mayu Tobin-Miyaji, *Assessing the Assessments: Maximizing the Effectiveness of Algorithmic & Privacy Risk Assessments*, EPIC (June 2025), https://epic.org/wp-content/uploads/2025/06/Assessing-the-Assessments-Report.pdf.

gone as well. Businesses should not have an opportunity to cure in these situations because the harm to consumers has already been done, so businesses should be held accountable for the harm they caused without an opportunity to cure. This is likely to be the case with most consequential decisions that are made using an ADMT under this law.

Additionally, much like the Colorado Privacy Act's repeal of its right to cure after January 2025, the Department should enact a sunset to this provision via the rulemaking process to require companies to comply with the law without receiving an unlimited get-out-regulation-free card.

EPIC, CFA, and Fairplay urge the Department to use their rulemaking authority and the discretion granted to them by this law to narrowly construe the right to cure and hesitate before allowing companies to take advantage of it.

II. Responses to Targeted Questions for Informal Input on the Chatbot Safety Act (Section V)

1. Definitions and Scope

a. Are the definitions of "conversational artificial intelligence service" and "operator" sufficiently clear? Would additional guidance or examples be useful? How might regulations provide guidance to ensure that these definitions are not interpreted too broadly or too narrowly? What are concerns if the definition is interpreted too broadly or too narrowly?

There is a significant risk that the definitions and other scoping criteria set forth in this law will not cover the most commonly harmful tools. The *twelve* exemptions to the already-limited definition of "conversational artificial intelligence service" are a compliance team's dream and could render this bill ineffective in practice.

In this definition, exemption I creates a squishy standard that could be used to exempt tools like ChatGPT, Meta, CharacterAI, Gemini, and others because these companies have always been described by others and themselves as both developers and researchers. For example, when ChatGPT was first released, it was described by both OpenAI and the media as a "research release" and a "research preview," and CharacterAI was developed by "researchers" from Google.[39] This exemption could quite easily be read to swallow the rule.

Similarly, exemptions II, IV, XI, and XII are particularly problematic because of the hyperbolic and sprawling way chatbot tools are advertised. Each of the biggest AI chatbot companies simultaneously advertise their tools as focused on educational opportunities,[40] as business tools to help make decisions to provide "commerce-related or transactional assistance,"[41] and as tools to be integrated into other software applications or web interfaces that are not themselves conversational AI services.

At the same time, exemption V is content-based, hard to guarantee, and creates significant concern around the voice chat interfaces that have caused concerning and negative outcomes.[42] Exemption VIII exempts theme parks from this chatbot protection bill and creates a worrisome potential gap for consumer protection that doesn't make sense. Especially because theme park-related tools are clearly likely to be primarily kid-focused, they should be subject to the provisions of this bill to ensure minors' safety, and the Department should consider removing this exemption.

Though the administration of health care arguably calls for some of the most stringent protections, as seen through other health privacy laws, exemptions IX and X exempt chatbots used in health care despite many of these tools being explicitly advertised and developed for such use.[43] The healthcare context is where some of the most sensitive use cases come up and is an area where any protections must be maintained and augmented. To allow for a gaping exception here poses a grave risk to consumers' health care and sensitive data. Existing health

---

[39] Lee Ying Shan & Jennifer Elias, *Google Gemini Co-Lead Noam Shazeer Leaves for OpenAI*, CNBC (Jun. 17, 2026), https://www.cnbc.com/2026/06/18/google-gemini-co-lead-noam-shazeer-leaves-for-openai.html; *Introducing ChatGPT*, OpenAI (Nov. 30, 2022), https://openai.com/index/chatgpt/.

[40] *Education: Microsoft 365 Copilot,* Microsoft, https://www.microsoft.com/en-us/education/products/copilot-in-education; *ChatGPT Edu: Bring AI to Campus at Scale*, OpenAI, https://chatgpt.com/business/education/.

[41] *Introducing Shopping Research in ChatGPT,* OpenAI (Nov. 24, 2025), https://openai.com/index/chatgpt-shopping-research/; *Shopping with Microsoft Copilot*, Microsoft, https://support.microsoft.com/en-us/microsoft-copilot/shopping-with-microsoft-copilot; *Compare Products Across Sites*, Claude, https://claude.com/resources/use-cases/compare-products-across-sites.

[42] R.J. Cross & Rory Erlich, *AI Comes to Playtime: Artificial Companions, Real Risks*, U.S. PIRG Education Fund (Dec. 2025), https://pirg.org/edfund/wp-content/uploads/2025/12/AI-Comes-to-Playtime-Artifical-companions-real-risks.pdf.

[43] *Chat GPT for Clinicians: Your Secure Clinical Reasoning Partner*, OpenAI, https://chatgpt.com/plans/clinicians/; Riley Griffin, *Meta AI Chief Sees Opportunity in Models' Giving Health Advice*, Bloomberg (Jun. 4, 2026), https://www.bloomberg.com/news/articles/2026-06-05/meta-ai-chief-sees-opportunity-in-models-giving-health-advice.

privacy laws are not in conflict with the provisions of this bill, so companies operating chatbots used in health care should be required to comply with both this law and existing laws regulating the industry.

Overall, the Department should use this rulemaking as an opportunity to clarify and carefully tailor the scope of these exemptions to prevent companies from exempting themselves from the law. Otherwise, the intent of the bill to protect Coloradans from chatbot harms falls flat.

b. Are there frameworks or other laws that the Department can look to in drafting regulations related to the definitions of these terms or others?

We recommend the Department look to the recently introduced federal People-First Chatbot Act as a guide.[44] The bill tackles the same issues that this law seeks to address, as well as many of the broader harms that we suggest addressing in this comment. The federal bill is largely based on a model chatbot bill developed by EPIC, CFA, and Fairplay to address chatbot harms.[45] While it has not yet passed in any state, it was introduced in seven states, had several hearings, and passed out of one committee.[46]

2. Considerations related to age determination

a. What factors should be considered in determining whether an age-estimation method is "commercially reasonable"? What evidence should be relevant in determining whether an operator has used commercially reasonable methods to estimate the age or age range of users? How should regulations account for changes in technology, industry practices, or the availability of age-estimation tools over time?

It is critical for the Department to ensure that age determination does not contribute to the commercial surveillance system and broader data protection crisis. By adopting both privacy-

---

[44] *See supra* note 6.
[45] EPIC, *People-First Chatbot Bill* (Dec. 2025), https://epic.org/people-first-chatbot-bill/.
[46] *See e.g.*, EPIC, *EPIC Urges Support for Chatbot Provider Liability Framework in Illinois* (May 5, 2026), https://epic.org/epic-urges-support-for-chatbot-provider-liability-framework-in-illinois/; EPIC, *EPIC Supports South Carolina Bills to Rein in Chatbot Harms* (Apr. 15, 2026), https://epic.org/epic-supports-south-carolina-bills-to-rein-in-chatbot-harms/; EPIC, *EPIC Testifies in Support of Maryland Chatbots Bill* (Mar. 13, 2026), https://epic.org/epic-testifies-in-support-of-maryland-chatbots-bill/. *See e.g.*, EPIC, *EPIC Urges Support for Chatbot Provider Liability Framework in Illinois* (May 5, 2026), https://epic.org/epic-urges-support-for-chatbot-provider-liability-framework-in-illinois/; EPIC, *EPIC Supports South Caroline Bills to Rein in Chatbot Harms* (Apr. 15, 2026), https://epic.org/epic-supports-south-carolina-bills-to-rein-in-chatbot-harms/; EPIC, *EPIC Testifies in Support of Maryland Chatbots Bill* (Mar. 13, 2026), https://epic.org/epic-testifies-in-support-of-maryland-chatbots-bill/.

and security-focused regulations, the Department can also incentivize the development of more secure and privacy-protective age determination technology.

The privacy risks from age determination vary not just from method-to-method but also from tool-to-tool as different companies have different data practices and implement different privacy and security features. In conjunction with the Data Protection Assessments that are already required under the Colorado Privacy Act, the Department should assess the privacy risks posed by each potential age determination tool and prioritize tools that minimize data collection, use, and disclosure. Currently, companies determine age using a range of tools, with some more privacy-protective than others. The user information an online age assurance tool collects, processes, and stores generally defines its privacy risks. The more personal information a company collects, processes, or stores—and the more sensitive that personal information—the higher the risk to users' privacy. But companies can implement privacy and security features that mitigate these risks, so the Department must look at the totality of a company's data practices and a tool's privacy and security features to determine the overall privacy risks.

The Department should require that any approved age determination tool only collect, process, and disclose personal information that is strictly necessary to determine whether a covered user is a covered minor. The regulations should also incentivize adoption and development of more privacy-protective and secure age determination technology in the future.

The Department should consider creating a formal process to incentivize the development and approval of new, privacy-protective age determination methods in the future. This process can be modeled off the Federal Trade Commission's (FTC) process to approve new Verifiable Parental Consent (VPC) methods for the Children's Online Privacy Protection Act (COPPA). The COPPA Rule lists several acceptable VPC methods but also invites operators or vendors to submit new VPC methods for FTC approval.[47] After a public comment period, the FTC can approve a new method that meets specific criteria set forth in the Rule: "Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[48]

---

[47] COPPA Rule, 16 C.F.R. § 312.5(b)(2) (2024), https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312/section-312.5.
[48] *Id.* § 312.5(b)(1).

The Department should institute a similar process in regulations to approve new, privacy-protective age determination tools in the future. The regulatory process for approving new methods should encourage the development of more secure and privacy-protective methods of determining age. The Department should consider the following factors when approving new age determination methods: the amount of personal information required to perform or transmit age determinations, whether the tool processes and stores age determinations on-device or in-browser, whether the tool uses privacy-protective communication techniques like zero knowledge proofs, whether the tool allows for once-and-done age determinations and has the potential to increase interoperability, and other privacy or data security features and risks.

3. <u>Reporting on suicide and self-harm response protocols</u>

a. What metrics should the Department consider including in the required annual reports to determine the efficacy and reliability of implemented safeguards or detection, removal, and response protocols? What metrics would be misleading or unreliable indicators of effectiveness? What information should operators provide specific to testing, validation, improvement, or monitoring of crisis-response systems?

The Department has the opportunity to require meaningful safety reports that would help researchers, well-meaning companies, and legislators make more informed decisions about both the decisions the chatbot companies are making on the moderation of their tools (i.e., what can be outputted by the tool) as well as to identify (in a non-identifiable/individual capacity to preserve privacy) the trends of what people are using the tool for.

The status quo is that the public and policymakers are forced to rely on self-reported numbers from the AI companies themselves, leading to fears that these companies may manipulate the benchmarks to make themselves look better and their chatbots look safer than they really are.[49] This is not reliable, not sustainable, and not acceptable for an industry that is

[49] *Meta Lied When Benchmark-Testing its Llama 4 Model*, Ohio Society of Ass'n Professionals (Jan. 9, 2026), https://www.ohiosap.org/news/meta-lied-when-benchmark-testing-its-llama-4-model; Justin Hart, *Why Every AI Benchmark Is Lying to You (And What that Actually Means)*, Hello, AI (Feb. 23, 2026), https://helloai.substack.com/p/why-every-ai-benchmark-is-lying-to.

causing significant harm.[50] The categories for reporting should be as quantitative and consistent as possible and should be made public in order to narrow the massive information and power asymmetry that currently exists between users and the deployers of the tools that are put in front of those users.

b. What information should be included in the online publication of data from these reports by the Department versus maintained confidentially by the Department?

While it is crucial that the Department make these reports and their accompanying data publicly available for researchers and legislators, protecting consumers and their privacy should remain the goal above all. As with other laws that mandate a method of accountability and transparency, compliance does not require sacrificing individual privacy.

In California, for example, the state's Companion Chatbot bill requires chatbot operators to report a series of metrics to the CPPA office, including the number of times the operator has issued a crisis service provider referral; protocols in place to detect, remove, and respond to instances of self-harm or suicidal ideation; and protocols in place to prohibit chatbot companions from responding in furtherance of suicidal ideations or actions by users, but it explicitly excludes any personal information about users or identifiers.[51] The Department's rulemaking should increase the accountability and transparency into how companies are responding to these serious risks to protect consumers and can safely do so without using consumers' personal information.

III. Conclusion

EPIC, CFA, and Fairplay applaud the Department's robust process to promulgate rules to protect consumers in accordance with existing Colorado law and both the Chatbot Safety Act and the Automated Decision-Making Technology Act. EPIC, CFA, and Fairplay will each continue

---

[50] *Generating Harms: Generative AI's Impact & Paths Forward*, EPIC (May 2023), https://epic.org/wp-content/uploads/2023/05/EPIC-Generative-AI-White-Paper-May2023.pdf; *Generating Harms II: Generative AI's New & Continued Impacts*, EPIC (May 2024), https://epic.org/wp-content/uploads/2024/05/EPIC-Generative-AI-II-Report-May2024-1.pdf.

[51] Companion Chatbots, Cal. Bus. & Prof. § 22603 (2025), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB243.

to be available for future discussion about our recommendations as to how the Department can best protect Coloradans.

Sincerely,

/s/ *Kara Williams*
Kara Williams
EPIC Counsel

/s/ *Stephanie Forbes*
Stephanie Forbes
EPIC Law Clerk

/s/ *Ben Winters*
Ben Winters
CFA Director of AI and Privacy

/s/ *Haley Hinkle*
Haley Hinkle
Fairplay Policy Counsel

/s/ *Brendan Bouffard*
Brendan Bouffard
Fairplay Staff Attorney