REGULATORY ANALYSIS FOR RULES GOVERNING THE

COLORADO PRIVACY ACT

January 20, 2023

Overview

The proposed Colorado Privacy Act Rules (the "Rules" or "CPA Rules") provide guidelines for covered businesses, non-profits, and government entities to implement the Colorado Privacy Act, Senate Bill 21-190 ("Concerning Additional Protection of Data Relating to Personal Privacy"), which was signed into law on July 8, 2021 (the "CPA" or the "Act"). The Colorado Department of Law ("Department") created the Rules to: 1) detail the technical specifications for one or more universal opt-out mechanism that will communicate a consumer's choice to opt out of the sale of personal data or processing of personal data for targeted advertising; and 2) clarify the ways in which covered organizations and entities carry out the CPA, simplifying compliance to create a protective, fair and efficient regulatory framework.

The Rules also clarify the obligations that covered entities have under the CPA, and create straightforward processes that will enable Colorado consumers to exercise their CPA rights. The Rules were drafted in response to provisions in the CPA directing the Colorado Attorney General to "adopt rules that detail the technical specification for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data", and permitting the Colorado Attorney General to "promulgate rules for the purpose of carrying out" the CPA.[1]

C.R.S. 24-4-103 (4.5)(a) and (c) state that, "upon request of any person…the agency shall issue a regulatory analysis of the proposed rule," and the analysis "shall be made available to the public at least 5 days prior to the rulemaking hearing." C.R.S. 24-4-103(4.5) requires the regulatory analysis to contain the following information:

1. A description of the classes of persons who will be affected by the proposed rule, including classes that will bear the costs of the proposed rule and classes that will benefit from the proposed rule;

2. To the extent practicable, a description of the probable quantitative and qualitative impact of the proposed rule, economic or otherwise, upon affected classes of persons;

3. The probable costs to the agency and to any other agency of the implementation and enforcement of the proposed rule and any anticipated effect on state revenues;

4. A comparison of the probable costs and benefits of the proposed rule to the probable costs and benefits of inaction;

5. A determination of whether there are less costly methods or less intrusive methods for achieving the purpose of the proposed rule; and

[1] C.R.S. § 6-1-1313.

6. A description of any alternative methods for achieving the purpose of the proposed rule that were seriously considered by the agency and the reasons why they were rejected in favor of the proposed rule.

C.R.S. 24-4-103 (4.5)(b) provides that "[e]ach regulatory analysis shall include quantification of the data to the extent practicable and shall take account of both short-term and long-term consequences."

1. **A description of the classes of persons who will be affected by the proposed rule, including classes that will bear the costs of the proposed rule and classes that will benefit from the proposed rule.**

The CPA aims to protect privacy by creating both privacy rights for Colorado consumers and obligations for entities that collect, maintain, and use large amounts of consumer personal data.[2] The CPA gives exclusive enforcement authority to the Colorado Attorney General (the "Attorney General") and Colorado District Attorneys.[3] The CPA Rules do not, themselves, create additional rights or obligations beyond those provided in the CPA, but attempt to clarify the CPA to both guide compliance and ensure that the Act is being carried out in a way that effectively provides Colorado consumers their privacy rights. As required, the CPA Rules also detail the technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data. Accordingly, the CPA rules will affect businesses and other entities that must comply with the CPA, as well as consumers.

A. Entities required to comply with the CPA

Entities required to comply with the CPA and CPA Rules may both bear costs and reap benefits of the Rules. Such entities will likely bear some cost in coming into compliance with the specific provisions of the Act together with the Rules. Importantly, regardless of whether the Department issues the CPA Rules, the entities must comply with the controller duties created by the CPA, such that many of the costs associated with compliance would exist either way.

Additionally, as discussed further below, the Rules provide definitions and standards that may benefit companies, lowering both overall compliance costs and costs associated with potential future enforcement by removing some uncertainty and ambiguity regarding the CPA's application and requirements. For instance, without concrete guidance, companies might guess at what compliance should look like and build a privacy program based on that guess, only to subsequently learn through enforcement that efforts taken were not sufficient or compliant. Knowing how to comply enables companies to avoid incurring such expenses.

[2] Specifically, the CPA applies to a Controller that "(a) conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and (b) satisfies one or both of the following thresholds: (i) controls or processes the personal data of one hundred thousand consumers or more during a calendar year; or (ii) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of twenty-five thousand consumers or more." C.R.S. § 6-1-1304. A "Controller" under the CPA means a person that, alone or jointly with others, determines the purposes for and means of processing personal data. C.R.S. § 6-1-1303(7).

[3] C.R.S. § 6-1-1311.

B. Consumers

The CPA was enacted, in part, to empower consumers to protect their privacy.[4] It does so by creating express consumer personal data rights that provide consumers with more transparency into and control over the way that businesses and other entities use their personal data. Those rights include a right to opt out of the processing of personal data for certain purposes, a right to access the personal data that a company collects and maintains about them, a right to delete personal data that a company maintains about them, and a right to obtain their data in a portable format.[5] While the CPA unambiguously intends for consumers to be able to exercise those rights, it provides little guidance as to how companies must make the rights available to consumers. Improper company compliance could offset the intended protections. For instance, if a consumer knows that they have a right to access their personal data, but a company creates a process that makes exercising the right to access unduly burdensome, the CPA's consumer rights become less meaningful and fail to empower consumers to protect their privacy as intended.

Accordingly, consumers benefit from rules that provide clarity and guidance as to how the CPA must be carried out. The CPA Rules discussed herein attempt to provide that clarity, ensuring that organizations tasked with providing consumer rights do so in a way that makes those rights accessible to and exercisable by Colorado consumers. For example, the CPA Rules provide guidance on how covered organizations and entities must disclose information to consumers in an understandable way, ensure that companies complying with the CPA do not make the rights request process burdensome for consumers attempting to exercise their rights, and explain what it means for entities to comply with data rights requests as well as obligations to safeguard personal data so that consumers have all of the rights and protection intended.

2. To the extent practicable, a description of the probable quantitative and qualitative impact of the proposed rule, economic or otherwise, upon affected classes of persons.

A. Entities required to comply with the CPA

The CPA applies to businesses, non-profits, and other entities based not on entity location, but instead on if they serve Colorado consumers and meet certain revenue or data processing thresholds. As such, it may apply to local, national, and international entities of a wide variety of sizes and businesses models. Direct and indirect costs to businesses and other entities required to comply with the CPA and related rules will vary considerably depending on the type of company, current privacy practices, business maturity, and number of Colorado consumers served by each entity. Additionally, many covered entities may have already built compliance programs for similar privacy regulations in Europe (the European Data Protection Regulations, "GDPR", which took effect in 2018) or California (the California Consumer Protection Act, "CCPA", which took effect in 2020). For example, the GDPR, CCPA, and CPA all require covered entities to honor consumer requests to access and delete their personal data. A 2021 survey found that 41% of businesses are very or fully compliant with the CCPA and 51% are very or fully compliant with the GDPR.[6] For entities that are already fully or partially compliant with the GDPR or

[4] C.R.S. § 6-1-1302(1)(c)(I)
[5] C.R.S. § 6-1-1306
[6] Müge Fazlioglu, *IAPP-EY Annual Privacy Governance Report 2021*, Intl. Association of Privacy Professionals (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4227244

CCPA, the Department anticipates lower compliance costs and increased efficiencies as they will be able to reuse data mapping, systems, and processes when complying with the CPA.

Third parties have estimated a wide range of potential costs to businesses and other entities to comply with the CPA and other similar privacy laws.[7] While the CPA gives the Attorney General both specific and broad rulemaking authority, most compliance costs will be incurred regardless of the adoption of specific rules. The statutory text of the CPA establishes the consumer rights and controller obligations that businesses and other entities must comply with, and which drive most costs. While the Rules clarify those statutory rights and obligations, they do not establish new compliance obligations beyond the scope of the Act. Indeed, the Rules provide definitions and standards that the Department believes may lower both overall compliance costs and costs associated with potential future enforcement by removing some uncertainty and ambiguity regarding the CPAs application and requirements.

Accordingly, the Department believes any specific costs required by the Rules, beyond the costs associated with the statutory requirements, are significantly less than the legal and compliance costs covered entities would incur were they to have to assess every statutory requirement without guidance or clarification from the Rules. For example, the Rules establish that the Department of Law will maintain a list of universal opt-out mechanisms that covered entities must accept, decreasing both uncertainty and costs associated with this statutory obligation. Similarly, the Rules offer details regarding the content of data protection assessments required by the CPA, making it more likely that covered entities can create these documents without the assistance of a third party. Additionally, the Department believes the direct costs to businesses and other entities is significantly outweighed by the benefit of protecting the public and consumers from the harms associated with use and abuse of private data.

While covered entities may anticipate short term negative revenue impacts to business models dependent on the use and sale of personal data, the long-term impact may provide a net increase in revenue. One study on the impact of the GDPR, focusing on the exercise of consumer consent and opt-out rights, found that while covered entities did see a reduction in total cookies tracked, the remaining cookies represented a more persistently trackable and engaged set of customers. This meant an initial decline in revenue for these companies, but over time the average value of the remaining consumers increased, offsetting losses from the consumers who opted out or did not consent.[8]

As consumers demand transparency and greater privacy protection from businesses and other entities, the Department believes businesses that respond to consumers with privacy protective practices will ultimately benefit through increased consumer trust and loyalty. Many companies have already begun to make data privacy a differentiator, with the top 10 most profitable companies in 2022 making public

[7] *See e.g.* Daniel Castro, et al, *The Looming Cost of a Patchwork of State Privacy Laws*, Information Technology & Innovation Foundation (2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/

[8] Guy Aridor, et al, *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*, National Bureau of Economic Research (Jan. 29, 2020),https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3522845

commitments to protect consumer privacy and security.[9] The CPA Rules will create consistency and clarity in privacy protective practices, benefiting the covered entities who must comply.

B. Consumers

The Colorado Legislature cited concerns about the "devastating impacts" of privacy harms as a key motivating factor for the Act.[10] The Rules will help protect Coloradans from concrete harm.

Economists connect data privacy harms to profound information asymmetries between individuals and the entities who collect and process information about them.[11] A large literature in behavioral economics demonstrates the way cognitive biases compound these problems, making people poor assessors of privacy risks.[12] These Rules will help individuals understand and control information held about them, decreasing these asymmetries and combatting these biases.

Although the Act is not merely about data breaches or identity theft, the Legislature pointed to "financial fraud" and "identity theft" as two of the key "devastating impacts" that motivated the Act. The Rules give Colorado consumers better control over their information – for example by exercising the rights to access, correct, and delete personal information, and the right to opt out of some uses of their information – in ways that might mitigate the economic costs of future data breaches. The Act also places obligations on covered entities to safeguard personal data and minimize their collection of data to what is reasonably necessary, which might also decrease these costs. Scholars have highlighted that the costs to consumers–and the broader economy–of data breaches include not only the direct costs of response but also significant costs stemming from fear and anxiety of ongoing negative impacts on finances and employment opportunities.[13]

Colorado consumers will also experience significant noneconomic benefits, which we factor into a comprehensive analysis of the impact of these Rules, even if such benefits cannot simply be compared quantitatively. Scholars identify privacy as an important condition for self-development, giving each of us what we need to navigate society and culture, starting from early childhood.[14] This development supports innovation as well, by giving would-be innovators the space they need to find "pathways of serendipity," that can be cut-off in a surveillance economy.[15]

Additionally, increased regulation of and consumer control over personal data may better protect consumers from both intentional and inadvertent discrimination. The development of new technology and platforms has offered novel opportunities to both businesses and consumers, but the use of personal data has also exposed users to potential harm. For example, sharing economy platforms that

[9] Dominique Shelton Leipzig, *How attention to data privacy will stabilize our financial markets*, Word Economic Forum (May 25, 2022), https://www.weforum.org/agenda/2022/05/how-attention-to-data-privacy-will-stabilize-our-markets/

[10] C.R.S. § 6-1-1302(1)(a)(V)

[11] Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. of ECON. LIT. 442 (2016).

[12] *See e.g.,* Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, ECONOMICS OF INFORMATION SECURITY 165, 172–73.

[13] Danielle Keats Citron & Daniel J. Solove , *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018).

[14] Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1911 (2013).

[15] Id. at 1927.

allow for race based discrimination through exposing personal information[16], companies collecting and selling or allowing access to sensitive sexual health and sexual orientation information[17], or algorithms leading to race based discrimination in housing and consumer-lending.[18] By limiting the use of certain kinds of personal data, requiring covered entities to evaluate potential harms, including discrimination, in both data collection and its use generally and in algorithms, and offering control and transparency to consumers, the CPA and Rules benefit consumers by offering additional and consistent protection from important civil rights related harms.

3. <u>The probable costs to the agency and to any other agency of the implementation and enforcement of the proposed rule and any anticipated effect on state revenues.</u>

Presently, there is no anticipated increase in the costs to the Department to administer or implement the Rules not already accounted for in the current and planned Department budget associated with enforcing the CPA and the Colorado Consumer Protection Act (CCPA). A violation of the CPA is considered an unfair trade practice under the CCPA. The Department already enforces the CCPA, which includes investigating and prosecuting unfair and deceptive trade practices. The Department does not anticipate requiring additional resources to implement and enforce the Rules. Further, an anticipated result of the Rules is to provide clarity regarding the scope of the CPA and compliance requirements, which should provide for more efficient investigation and enforcement by the Department.

4. <u>A comparison of the probable costs and benefits of the proposed rule to the probable costs and benefits of inaction.</u>

<u>A. Public Benefits</u>

The Rules are designed to implement the CPA, and the CPA promotes substantial and real economic benefits to the public at large. The Rules will assist the Department of Law in enforcing the CPA and

---

[16] *See e.g.,* Jasper Dag Tjaden, et al, *Ride with Me – Ethnic Discrimination, Social Markets and the Sharing Economy*, 34 EUROPEAN SOCIOLOGICAL REVIEW 418 (2018); Benjamin Edelman and Michael Luca, *Digital Discrimination: The Case of Airbnb.com*, Harvard Business School Working Paper No. 14-054 (2014), https://www.hbs.edu/ris/Publication%20Files/Airbnb_92dd6086-6e46-4eaf-9cea-60fe5ba3c596.pdf; Sara Clemence, *Black Travelers Say Home-Share Hosts Discriminate, and a New Airbnb Report Agrees*, N.Y. TIMES (Dec. 13, 2022), https://www.nytimes.com/2022/12/13/travel/vacation-rentals-racism.html; Taylor Kubota, *Researchers from Stanford, MIT and the University of Washington find ride-share drivers discriminate based on race and gender*, STANFORD NEWS (Oct. 31, 2016), https://news.stanford.edu/2016/10/31/researchers-stanford-mit-university-washington-find-ride-share-drivers-discriminate-based-race-gender/

[17] *See e.g.,* Scott Neuman and Camila Domonoske, *Grindr Admits It Shared HIV Status Of Users*, NPR (Apr. 3, 2018), https://www.npr.org/sections/thetwo-way/2018/04/03/599069424/grindr-admits-it-shared-hiv-status-of-users; Sara Morrison, *This outed priest's story is a warning for everyone about the need for data privacy laws*, VOX (Jul. 21, 2021), https://www.vox.com/recode/22587248/grindr-app-location-data-outed-priest-jeffrey-burrill-pillar-data-harvesting; Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood; Queenie Wong, *Facebook Reportedly Collects Data About Abortion Seekers*, CNET (Jun. 15, 2022), https://www.cnet.com/news/social-media/facebook-reportedly-collects-data-about-abortion-seekers/

[18] Robert Bartlett, et al, *Consumer-Lending Discrimination in the FinTech Era*, 143 J. of FINANCIAL ECON. 30 (2022); Press Release, Department of Justice, Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising (Jun. 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known

support the Attorney General's mandate to protect the public and businesses from activity which threatens consumers and the marketplace. Given that the CPA is designed to protect consumers from the financial, personal, emotional, and physical harms discussed earlier and that accompany the increased collection of personal data, rules which advance these goals will economically benefit society by both decreasing these harms and increasing consumer confidence in transactions where their data may be collected and used.

Absent implementation of the Rules, the Department may face delays in and increased cost of enforcement caused by confusion among covered entities. As noted earlier, the proposed Rules will streamline and create consistency among both the implementation and enforcement of the CPA. This will also increase economic competitiveness for covered entities that are not violating the CPA. Additionally, ensuring expeditious enforcement will further benefit the public by more quickly identifying and ceasing activity in violation of the CPA.

B. Market Benefits

Privacy and privacy protective technology is a growing industry in both the United States and internationally.[19] The CPA rules will permit economic growth and create jobs contributing to the already growing market for technical, legal, customer service, and information security professionals well versed in privacy best practices and data management. Even before the CPA and other US privacy laws have taken effect, businesses report growing their privacy teams by an average of 12% in 2022[20] and one report estimates a 30% increase in data privacy jobs in 2021, with the trend projected to continue.[21] The CPA and rules will also stimulate innovation and job growth in Colorado as new businesses emerge to help covered entities comply with the regulations and assist consumers with enacting their rights.

The CPA and the Rules will allow Colorado companies to compete and grow their customer base on a national and international scale as compliance with the CPA and the Rules will make it easier to comply with, and operate in, additional markets with similar privacy requirements.[22] As consumer concerns regarding the collection and privacy of their personal data grow, the Department believes the CPA and

[19] Gené Teare, *Almost $10B Invested In Privacy And Security Companies In 2019*, CRUNCHBASE NEWS (Jan. 29, 2020), https://news.crunchbase.com/venture/almost-10b-invested-in-privacy-and-security-companies-in-2019/; Press Release, Acumen Research and Consulting, Data Privacy Software Market To Garner US$ 35,088 Million Revenue By 2030 Growing at CAGR 40.2% (Aug. 23, 2022), https://www.globenewswire.com/en/news-release/2022/08/23/2503415/0/en/Data-Privacy-Software-Market-To-Garner-US-35-088-Million-Revenue-By-2030-Growing-at-CAGR-40-2-Exclusive-Report-by-Acumen-Research-and-Consulting.html#:~:text=Data%20Privacy%20Software%20Market%20Report,of%2040.2%25%20from%202022%2D2030.

[20] *IAPP-EY Annual Privacy Governance Report 2022*, International Association of Privacy Professions (2022), https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2022_Executive_Summary.pdf)

[21] *2022 Data Privacy Jobs Report*, Tru Staffing Partners (2022), https://info.trustaffingpartners.com/2022-data-privacy-jobs-report

[22] As of January 2022, 137 out of 194 countries had put in place legislation to secure the protection of data and privacy. UNCTAD, *Data Protection and Privacy Legislation Worldwide*, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

the Rules will both establish Colorado as a leader in privacy protection and promote economic growth and create new jobs.

Additionally, research has demonstrated that privacy regulation can be pro-competitive. While some have argued that increased privacy regulation could stifle innovation by raising the cost of entering a market, privacy regulation may also reduce the power of incumbents by limiting the advantages they gain from amassing large amounts of consumer personal data. For example, in one recent empirical study examining the impact of the GDPR on the iOS mobile application market, research found that for free mobile apps, which often rely more heavily on the use and sale of personal data, the increased privacy regulations from the GDPR also increased competition.[23] Specifically, GDPR privacy regulations resulted in more new apps in the free apps top charts and increased rank volatility – demonstrating an increased ability for new apps to compete with incumbents.[24] While the impact of the CPA Rules and privacy regulation more broadly may vary by market and business model, the Department believes that creating a level playing field for the collection and use of data will offer new market entrants and new business models increased opportunities for competition and reduce the power of incumbents who have already compiled large amounts of data.

C. Costs of Inaction

As discussed in various other sections of this analysis, inaction would deprive the public, and the economic market of the benefits discussed above, lead to higher compliance and enforcement costs, and potentially offset the protective value of the CPA for Colorado consumers.

The CPA provides concrete rights and obligations without explanation of how entities must provide those rights and comply with their obligations. Absent clarification and guidance, entities will face the expense of assessing each statutory requirement and guessing at proper compliance. Enforcement would be similarly challenging if the Attorney General and district attorneys had to assess privacy programs that were created without any guiding standards. The compliance standards set forth in the CPA Rules provide clarity for covered organizations and create benchmarks for efficient and fair enforcement. For example, the CPA prohibits complying entities from using dark patterns to obtain consent, without defining "dark patterns". Without guidelines and standards relating to dark patterns, complying entities would be left to guess at which consent interfaces contain dark patterns, and enforcers would have to assess every single consent interface to determine whether it contains dark patterns without any guidance or accepted standards, potentially leading to costly litigation.

Additionally, without the guidance of the CPA Rules, organizations could create processes that overburden consumers seeking to exercise their rights, place obstacles around consumer rights, provide required information in unintelligible forms, and ultimately offset protections provided by the CPA. For example, the CPA provides a right for consumers to access the personal data that a covered organization collects about them. Consumers in other jurisdictions with comprehensive privacy laws containing similar rights have expressed that companies serving consumers in those jurisdictions were responding to requests to exercise a similar right to access with completely unintelligible and useless information

[23] Xi Wu and Min-Seok Pang, *How Data Privacy Regulations Affect Competition: Empirical Evidence from the Mobile Application Market*, Proceedings of the 42nd Intl. Conf. on Info. Systems (2014).
[24] *Id.*

that did not actually give consumers an understanding of the personal data collected.[25] To prevent a similar outcome in Colorado, the CPA Rules clarify that responses to consumer requests to exercise the right to access must be "provided in in a form that is concise, transparent and easily intelligible and available in the language in which the Consumer interacts with the Controller."[26]

As such, the CPA Rules are necessary to ensure that the CPA is given full effect and provides the protection and consumer transparency and control intended.

5. A determination of whether there are less costly methods or less intrusive methods for achieving the purpose of the proposed rule.

The Department has considered the alternatives below, as well as inaction, and determined that there is no less costly or less intrusive method for achieving the purpose of the proposed Rules.

6. A description of any alternative methods for achieving the purpose of the proposed rule that were seriously considered by the agency and the reasons why they were rejected in favor of the proposed rule.

To clarify CPA requirements and create guidelines for both complying entities and consumers, the Department of Law considered the following alternative methods:

(1) Waiting to Issue permissive rules under C.R.S. § 1313(1) until the July 1, 2025, deadline associated with specific opinion letter and interpretive guidance rules under C.R.S. § 1313(3).

(2) Issuing limited opinion letter and interpretive guidance rules contemplated in C.R.S. § 6-1-1313(3) now and using interpretive guidance rules to provide clarity about the application of the CPA as questions arise.

These options would further complicate compliance by decreasing the understanding of the CPA at the time it takes effect and adding uncertainty for covered entities as they build compliance programs. Covered entities would have to spend additional resources interpreting the CPA once it goes into effect and might incur further costs making changes to their compliance program when regulations were released later. Consumers could also face inconsistency with how the CPA will be implemented, making it harder for such consumers to exercise their privacy rights.

[25] Colorado Privacy Act Public Input Session, June 28, 2022, available at https://www.youtube.com/watch?v=ivhHwwsNe48

[26] 4 CCR 904-3, Rule 4.04(B)(2).