November 8, 2021

Via Email

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814
regulations@cppa.ca.gov

RE: Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2021 (PRO 01-21)

Dear Ms. Castanon:

The Entertainment Software Association ("ESA")[1] submits these comments in connection with the California Privacy Protection Agency's ("CPPA") preliminary efforts to implement regulations under the California Privacy Rights Act ("CPRA").[2]

ESA respectfully requests that the CPPA adopt regulations that:

- Discourage fraudsters and other bad actors from attempting to use the correction right to undermine the security or integrity of the service or facilitate their unlawful or malicious conduct.
- Ensure that any technical specifications for the voluntary opt-out preference signal are consistent with existing children's privacy laws and reliably convey a parent's or user's choice.
- Provide consumers meaningful access to personal information, while maintaining the safety, security, and integrity of the business's services.
- Clarify what constitutes "dark patterns" and "precise geolocation" information to align with the Federal Trade Commission's precedent and guidance.
- Consistent with the statutory text, specify that consumers can opt out of automated decisionmaking only where such data processing uses or discloses sensitive personal information, and ensure that disclosing meaningful information about the logic of such data

[1] ESA is the U.S. association for companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the internet. There are over 400 video game companies in the state of California.

[2] California Privacy Protection Agency, Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Sept. 22, 2021), https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

processing does not adversely impact intellectual property rights or efforts to detect and prevent fraud or other malicious conduct.

We explain each of these requests in more detail below.

I. The regulations should discourage fraudsters and other bad actors from attempting to use the correction right to undermine the security or integrity of the service or facilitate their unlawful or malicious conduct.

In the experience of ESA's members, fraudsters and other bad actors can abuse correction rights to try to evade detection, gain unauthorized access to an account, or otherwise facilitate their unlawful or malicious conduct. For example, a video game player who has been banned from an online game for harassing other players or cheating in violation of the game's terms of use might attempt to request "correction" of their IP address, username, or other personal information in order to try to circumvent the game company's anti-fraud, anti-cheat, and other detection systems that prevent such players from attempting to create new accounts. Malicious actors also may try to use the "correction" right to try to make it easier to gain unauthorized access to another user's account or regain access to a fraudulent account. To discourage such efforts, the regulations should make clear that where a business has a reasonable belief that the particular consumer is attempting to abuse the correction right for malicious purposes, it may deny correction requests in order to prevent fraud, including requests that would undermine the security or integrity of the service or facilitate unlawful or otherwise malicious conduct.

Specifically, ESA requests that the CPPA include the following in its CPRA regulations:

> ***Nothing in these regulations shall restrict a business's, service provider's, third party's, or contractor's ability to: prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive conduct, or any unlawful activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action.***[3]

Such language is necessary to maintain consistency with the plain text and clear intent of the CPRA, which allows businesses to deny requests that are not "verifiable" and also recognizes the need to balance the rights of consumers with the need to protect others and discourage unlawful activity.[4] It

[3] This language is consistent with other state laws that empower businesses to protect consumers from fraudulent and malicious conduct. *See, e.g.*, Virginia Consumer Data Protection Act 59.1-578(A)(7); Colorado Privacy Act 6-1-1304(3)(A)(X).

[4] *See, e.g.*, CPRA §§ 1798.106(c) (requiring businesses to correct personal information in response to a verifiable consumer request only); 1798.185(a)(8)(C) (balancing the correction right against the need to prevent fraud); 1798.185(a)(8)(B) (balancing the correction right against the need for accuracy); 1798.145(a)(3) (recognizing that the correction right does not restrict a business's ability to cooperate with law enforcement agencies regarding conduct that the business has a good faith belief is illegal); 1798.145(a)(5) (preventing correction where it would limit a business's ability to exercise or defend against legal claims); 1798.145(k) (recognizing that the correction right should not adversely affect the rights and freedoms of others); 1798.140(ac) (recognizing the need to protect system "security and integrity").

also is supported by the existing text of the California Consumer Privacy Act ("CCPA") regulations and the commentary that the California Attorney General published when issuing those regulations.[5]

II. The regulations should ensure that any technical specifications for a voluntary opt-out preference signal are consistent with existing children's privacy laws and reliably convey a parent's or user's choice.

The CPRA's voluntary opt-out preference signal has the potential to provide an innovative new mechanism for consumers to exercise their CPRA rights and for businesses to have flexibility in how they choose to provide notice about and respond to consumers' opt-out requests. However, whether this mechanism succeeds or fails depends in large part on whether it proves reliable in accurately conveying the person's intended choice and avoids conflicting with other consent mechanisms.

Ensuring reliability and avoiding conflicting consent mechanisms is especially critical with respect to consumers who are under the age of 13, because any technical specifications for a voluntary opt-out preference signal must be carefully designed to ensure consistency with the Children's Online Privacy Protection Act ("COPPA"). Any business whose online service is directed to children under 13 or that has actual knowledge that it collects personal information online from California consumers younger than 13 years of age must also comply with COPPA. COPPA preempts any action by a state or local government that imposes "any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in [COPPA] that is inconsistent with the treatment of those activities or actions under [COPPA]."[6]

To ensure consistency with COPPA, the CPRA regulations must require businesses to honor any preference signal for children under 13 years old only if such signal satisfies COPPA's standard for

[5] *See, e.g.*, Cal. Code Regs. Tit. 11, §§ 999.314(c)(4) (permitting service providers to use personal information for security and anti-fraud purposes); 999.315(g) (allowing a business to refuse fraudulent opt-out requests); 999.323(c) (authorizing the collection of additional information during the verification process for security and fraud-prevention purposes); California Department of Justice, Initial Statement of Reasons, at 29, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf [hereafter, "ISOR"] (noting that the regulations require "a business to consider a variety of factors in determining the verification method, such as . . . the likelihood that fraudulent or malicious actors are seeking the information"); ISOR, 31 (explaining that the regulations "provide clear direction that the business should prioritize security and fraud-prevention over disclosure"); California Department of Justice, Final Statement of Reasons, at 19, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf [hereafter, "FSOR"] (explaining that the verification process is for "minimizing the risk of fraud or malicious activity"); FSOR, 34 (explaining that the regulations permit service providers to use personal information "to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity"); FSOR, Appendix A, Row 744, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf [hereafter "Appendix A] (explaining that the regulations require "businesses to not comply with a consumer's request if it suspects fraudulent or malicious activity"); ISOR, 44 ("Given the wide variety of different industries subject to the CCPA, prescribing a particular method of verification may not provide the flexibility necessary to address all the different circumstances in which businesses and consumers interact, nor would it address changing data security standards and evolving technologies.").

[6] 15 U.S.C. § 6502(d).

"verifiable parental consent." Under COPPA, parents must provide "verifiable parental consent" before a business may collect, use, or disclose online the personal information of children under 13 years old, unless one of COPPA's various exceptions applies.[7] Importantly, COPPA requires that the parent's choices be "verifiable," and the COPPA statute and more than a decade of Federal Trade Commission guidance make clear that the standard is a high bar for ensuring that it is the child's parent or legal guardian who is exercising the choice.[8] Consequently, to ensure consistency with COPPA, the CPRA regulations must not require a business whose online service is child-directed or that has actual knowledge that it collects personal information from a child under the age of 13 to respond to the preference signal unless the signal constitutes "verifiable parental consent" as that term is defined in COPPA.

In addition, the CPRA regulations must not require businesses to honor any preference signal for children under 13 years old from an authorized agent of a parent or legal guardian. Under COPPA, only parents and legal guardians may exercise the right to consent (or withdraw consent) for the online collection, use, or disclosure of their child's personal information.[9] Consequently, the CPRA regulations must not require a business whose online service is child-directed or that has actual knowledge that it collects personal information from a child under the age of 13 to respond to a preference signal from any authorized agent who does not appear to be the parent or legal guardian of the child.

The invitation for preliminary comment also specifically asks "what technical specifications should be established for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age."[10] Because any technical specification that signals age would contradict clear, long-established Federal Trade Commission ("FTC") guidance and ultimately is likely to prove too unreliable to effectively promote the CPRA's goals, ESA requests that the CPRA regulations not include any such technical specification. The FTC has long held that websites and online services that are primarily directed to children under 13 must presume that all users are under the age of 13 and cannot

[7] *Id.* § 6502(a); 16 C.F.R. § 312.5.

[8] *See, e.g.*, ISOR, 34 ("The requirement of a 'reasonable method' is based on the similar requirement in the Children's Online Privacy Protection Act (hereinafter COPPA) (15 U.S.C. § 6501, et seq.). . . . The methods are the same as those set forth in regulations issued by the Federal Trade Commission in furtherance of COPPA[.]"); Appendix A, Row 798 ("Section 999.330(a)(2) has been modified to clarify that acceptable methods are not limited to the ones listed in the regulations."); 15 U.S.C. §§ 6501(9), 6502(b); 16 C.F.R. § 312.5.

[9] 16 C.F.R. § 312.2 (defining "parent" to include a legal guardian); 15 U.S.C. § 6501(9) (defining "verifiable parental consent" to be "any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that ***a parent of a child*** receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.")(emphasis added).

[10] CPPA, *supra* note 2, at 4.

age gate.[11] The proposal would appear to conflict with this approach by allowing business that operate primarily child-directed sites or services to rely on the purported age conveyed through the preference signal to determine whether a parent or the child can exercise the applicable rights over use or disclosure of personal information. The proposal also would appear to conflict with the FTC's guidance on age screens.[12] Families often use shared devices across a household, particularly in the context of video gaming. For example, a parent may install a video game on their mobile phone, tablet, or personal computer and then hand that device over to their child to play. If an adult previously set a preference signal for that device, that default would presumably continue to apply even though COPPA requires neutral age screen mechanisms without defaults. If the preference signal was changed to indicate that the user is under 13 and is subsequently changed back to indicate an older age, it would be impossible to know whether that change was done by the parent or the child. Such a result is inconsistent with the FTC's guidance, which recommends using technical means "to prevent children from back-buttoning to enter a different age."[13]

Because purported age information delivered via preference signal is likely to be so unreliable, it creates a significant risk that companies will receive conflicting age information from the user or their parent or guardian. Importantly, the FTC has repeatedly reiterated that businesses (including, but not limited to, general audience sites) have no duty to investigate age,[14] so any regulations that would, in effect, create such a duty to resolve conflicts between the age a user or their parent or guardian provides during account creation and the age indicated through the preference signal (which could potentially change repeatedly over time and as described above, would not be reliable evidence of a user's actual age) would be inconsistent with COPPA.[15] For example, when a parent creates an account for their child with the provider of a video game console or a video game publisher, they may provide the child's date of birth and (if that child is under 13) grant verifiable parental consent consistent with COPPA to the requested online collection, use, and disclosure of the child's personal information. If that child is subsequently playing the game but conflicting age information is provided through the preference signal, this conflict makes the business's obligations under the CPRA unclear. It is also not clear how a parent or legal guardian could exercise different opt-out preferences if they have multiple children under 13 years of age, or how different preferences could be communicated for these young children, the parents themselves, and other children in the household who might be at least 13 years of age, absent the collection of more personal information than may otherwise be needed to provide the

[11] *See, e.g.*, FTC, *Complying with COPPA: Frequently Asked Questions*, at H.2 (July 2020) [hereinafter "COPPA FAQ"], available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.

[12] *See id.* at D.7.

[13] *Id.*

[14] *See, e.g.*, COPPA FAQ, at E.2; 76 Fed. Reg. 59804, 59806 (stating that operators need not "ferret through a host of circumstantial information to determine who may or may not be a child").

[15] Notably, the FTC previously has encouraged the development of a technical specification to allow operators of child-directed sites and services to signal their status to third parties (such as social media plug-ins and ad networks) to facilitate COPPA compliance. Unlike such a signal, which can convey a static, reliable fact (i.e., that the particular website address is child-directed), purported age information (which varies over time and across individuals) cannot be reliably and effectively conveyed using a preference signal.

requested services. Such a fundamental paradigm shift away from a free and open internet with room for anonymous speech to an identity-based internet requiring verification for all online activity does not appear to have been contemplated or intended under the CPRA.

III. The regulations should require businesses to provide consumers with meaningful information while also permitting them to maintain the safety, security, and integrity of their services and systems.

The regulations should carefully balance the need to provide consumers meaningful access to the personal information they provide and the need to maintain the safety, security, and integrity of the service and systems.

Specifically, video game companies should not be obligated to return system logs, technical gameplay data, and similar technical data in response to a consumer's access request. As a threshold matter, this data generally is not personal information. Moreover, the CPRA specifies that businesses must provide only the "specific pieces of personal information obtained from the consumer" in response to access requests.[16] The text "from" is plain that only personal information that the consumer provides directly is subject to this access right. System logs, technical gameplay data, and similar technical data is automatically generated by the business, and is not "from" the consumer. Such data also often includes trade secrets,[17] and malicious actors may be able to use it to undermine a business's efforts to detect and prevent security incidents, cheating, fraud, and other unlawful or malicious activity.[18]

For these reasons, ESA respectfully requests that the CPPA include the following provision in its regulations:

> ***Nothing in these regulations shall require businesses to provide consumers with access to system logs and similar technical data,***

[16] CPRA § 1798.130(a)(3)(B)(iii).

[17] *Id.* at § 1798.185(a)(3) (requiring regulations to establish "any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request").

[18] *Id.* at §§ 1798.130(a)(3)(B)(iii) (specifying that "'specific pieces of information' do not include data generated to help ensure security and integrity"); 1798.140(ac) (defining "security and integrity" as "the ability: (1) of a network or an information system to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information; (2) to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions, and to help prosecute those responsible for such actions; and (3) a business to ensure the physical safety of natural persons"); *see also* Cal. Code Regs. Tit. 11 § 999.313(c)(4) ("A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics.").

> ***automatically generated data, or any data used for security and integrity purposes.***[19]

IV. The regulations clarifying "dark patterns" should align with the Federal Trade Commission's longstanding precedent and guidance on unfair or deceptive practices.

The CPRA's current "dark patterns" definition, which determines when a user's consent is effective for purposes of the CPRA, is vague. Accordingly, the CPPA should clarify in its regulations what consent practices constitute dark patterns by incorporating and aligning with existing FTC precedent and guidance. The CPRA defines dark patterns as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation."[20] This definition creates ambiguity because key concepts—such as "substantial," "subversion," and "autonomy"—are nebulous. The definition's vagueness potentially chills constitutionally-protected commercial speech, since such speech is designed to affect individuals' decisionmaking.

The ESA therefore urges the CPPA to enact regulations that clarify the CPRA's "dark patterns" definition by incorporating and aligning with the FTC's robust taxonomy of user interface designs that the FTC has deemed are unlawful as unfair or deceptive practices. Over the last forty years, the FTC has issued various guidance on unlawful disclosure and design practices and enforced against companies that sought to deceive consumers through such practices. As illustrated throughout its prior enforcement actions and guidance, the FTC has identified the following practices as unlawful: (1) buried language that obscures material disclosures in terms;[21] (2) poorly-labeled hyperlinks that hide material terms from consumers;[22] (3) trick language that confuses consumers;[23] and (4) bait and switch practices.[24] The CPPA should clarify the CPRA's definition by specifying that these practices constitute

[19] CPRA § 1798.130(a)(3)(B)(iii) (specifying that the specific pieces of information that must be provided in response to an access request do not include "data generated to help ensure security and integrity or as prescribed by regulation").

[20] CPRA § 1798.140(l).

[21] FTC, *.com Disclosures: How to Make Effective Disclosures in Digital Advertising*, at 10, 18 (2013) [hereinafter "*.com Disclosures Guidance*"].

[22] *See, e.g., id.* at ii (explaining that hyperlinks should provide access to disclosures that are not integral to the claim and should be labeled in a way that conveys the type and import of information to which they lead if clicked); Complaint, *FTC v. Vizio, Inc.* (Feb. 6, 2017) ("The notification provided no information about the collection of viewing data or ACR software. Nor did it directly link to the settings menu or privacy policy.").

[23] *See, e.g.*, *.com Disclosures Guidance*, at Appendix (detailing twenty-two examples of clear and unclear disclosures); Press Release, *Rent-To-Own Payment Plan Company Progressive Leasing Will Pay $175 Million to Settle FTC Charges It Deceived Consumers About Pricing* (2020); Complaint, *In re* Facebook Inc. (Aug. 10, 2012); Complaint, *In re* PayPal, Inc. (May 24, 2018).

[24] *See, e.g.*, FTC, *Advertising FAQ's: A Guide for Small Business* (2001); *Guides Against Bait Advertising*, 16 C.F.R. § 238.0 (2012); Press Release, *Abating Bait-and-Switch Buyback Tactics for Devices* (2016); Press Release, *The Lead-Generation Bait-and-Switch* (2019); FTC, *Native Advertising: A Guide for Businesses* (2015).

dark patterns and that therefore consent is not effective under the CPRA when businesses obtain consent using such unlawful practices.[25]

V. The regulations to further define precise geolocation should be informed by the FTC's guidance.

Any regulations that further define precise geolocation information should be consistent with and informed by how the FTC has defined and interpreted that term in its guidance and prior enforcement actions.

The CPRA currently defines precise geolocation as "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations."[26] The CPRA also recognizes that personal information that reveals "precise geolocation" is a type of sensitive personal information, thereby giving consumers the right to limit its use and disclosure in certain circumstances.[27]

While the FTC similarly has interpreted precise geolocation information to be data that is derived from a device (based, for example, on GPS, WiFi, or cell-tower data), the FTC has not imposed any arbitrary geographic radius based on this location. Because the proposed definition of "precise geolocation" is inconsistent with how that term has been interpreted and applied by the FTC, it could create consumer confusion regarding the scope or meaning of privacy settings or representations related to precise geolocation information.[28] Accordingly, ESA respectfully requests that the CPPA adopt the following language in its final regulations to align with the FTC's definitions of precise geolocation information:

> ***"Precise geolocation" means any data that is derived from a device (including GPS, WiFi, or cell tower) and that (1) is used or intended to be used to locate a consumer and (2) is sufficient to identify street name and name of city or town.***

[25] CPRA §§ 1798.140 (specifying that "agreement obtained through use of dark patterns does not constitute consent"); 1798.185(20) (specifying that links to a webpage or supporting content "that allows the consumer to consent to opt-in [shall not] make use of any dark patterns").

[26] CPRA § 1798.140(w).

[27] *Id.* at §§ 1798.140(ae)(1)(C), 1798.121.

[28] COPPA FAQ, at G.3 ("The Rule covers 'geolocation information sufficient to identify street name and name of city or town.'"); *see also* Decision and Order, *In re* Goldenshores Technologies LLC (F.T.C. Mar. 31, 2014), available at https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf ("precise geolocation data of an individual or mobile device, including but not limited to GPS-based, WiFi-based, or cell-based location information"); Decision and Order, *In re* Uber Technologies Inc. (F.T.C. Oct. 25, 2018), available at https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf; Stipulated Order for Permanent Injunction and Civil Penalty Judgment (same).

VI. Any opt-outs with respect to automated decisionmaking technologies should align with the statutory text as well as efforts to protect the safety of consumers and intellectual property rights.

Consistent with the CPRA's text, the regulations should provide consumers with the ability to opt out of automated decisionmaking technology that uses or discloses sensitive personal information. Additionally, the regulations should balance giving consumers access to information about automated decisionmaking technology with the need to protect consumer safety and intellectual property rights.

A. *The regulations should permit consumers to opt out of automated decisionmaking technology that uses or discloses sensitive personal information.*

The CPRA expanded the scope of the CCPA to provide consumers specific new opt-out rights—namely to opt out of the sharing of personal information for cross-context behavioral advertising and the right to opt out of certain uses and disclosures of sensitive personal information.[29] Notably, the statute did *not* create a blanket right to opt out of all automated decisionmaking technologies.[30] Accordingly, the CPPA's authority to issue regulations related to automated decisionmaking opt-outs is limited to interpreting the scope and application of the existing statutory opt-out rights.

The consumer opt-out right that most closely relates to automated decisionmaking technology is the right to limit the use and disclosure of sensitive personal information. Significantly, automated decisionmaking technology includes "profiling," which is defined to include sensitive processing concerning the consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.[31] This interpretation is further supported by the fact that these "profiling" activities generally track the types of personal information that are "sensitive" under the CPRA, including union membership (a type of information concerning work performance); financial account information (concerning the consumer's economic situation); genetic and health data (concerning the consumer's health); personal preferences and interests data (concerning the consumer's religious or philosophical beliefs), behavioral data (concerning sex life), and precise geolocation (concerning a consumer's location or movements).[32] Accordingly, ESA respectfully requests that the CPPA adopt regulations that state the following:[33]

[29] CPRA §§ 1798.120 (opt-out of sharing); 1798.121 (limit the use and disclosure of sensitive personal information).

[30] Appendix A, Row 17 ("The OAG cannot implement regulations that alter or amend a statute or enlarge or impair its scope."); *see also People v. K.P.*, 30 Cal. App. 5th 331, 341, 241 Cal. Rptr. 3d 324, 331 (2018) ("The failure of the Legislature to change the law in a particular respect when the subject is generally before it and changes in other respects are made is indicative of an intent to leave the law as it stands in the aspects not amended.") (internal quotations omitted).

[31] CPRA § 1798.140(z).

[32] *Id.* § 1798.140(ae).

[33] In addition, the CPRA's blanket statutory exemptions would apply with respect to this right as well. *See, e.g.,* CPRA § 1798.145.

> ***A consumer may request to opt out of a business's use of automated decisionmaking technology to the extent such technology uses or discloses the consumer's sensitive personal information.***

In addition to ensuring that the regulations are consistent with the text and purpose of the CPRA statute, the above approach also harmonizes the CPRA with international standards governing automated decisionmaking technologies. For example, Article 22 of the EU General Data Protection Regulation provides individuals the right to avoid being subject to automated decisionmaking, including profiling, where it "produces legal effects concerning him or her or similarly significantly affects him or her."[34] Interpreting the CPRA's automated decisionmaking opt out to apply to the extent such technology uses or discloses the consumer's sensitive personal information would result in similarly scoping this right to automated decisions that are likely to produce legal or similarly significant effects.

B. Disclosures of meaningful information about automated decisionmaking logic should be consistent with the statutory text and not adversely impact intellectual property rights or efforts to combat malicious conduct.

We support the CPRA's goal of providing consumers meaningful information about the logic used for automated decisionmaking technologies. As explained above, however, such rights should be aligned with the statutory text's focus on automated decisionmaking technologies that use or disclose sensitive personal information and therefore risk having a legal or similarly significant effect on the consumer. Moreover, the CPRA regulations should provide businesses flexibility to disclose meaningful information to consumers, while balancing the need to protect intellectual property rights and to prevent fraud and other malicious conduct. Depending on the sensitivity of the automated decisionmaking process and the types of personal information used, this could include, for example, providing a general explanation of how the automated decisionmaking process functions, the purposes for which such process is used, and the types of data or sources of personal data such process uses. The California Attorney General adopted a similar approach when that office issued regulations requiring privacy policies to include only a "general description" of verification processes. The California Attorney General explicitly recognized that businesses should not have to provide bad actors with a blueprint to evade their verification processes.[35]

Accordingly, ESA respectfully requests that the CPPA include the following language in the CPRA regulations:

> ***A consumer may request to receive meaningful information about the logic of automated decisionmaking technology that uses or discloses the consumer's sensitive personal information. In responding to such a***

[34] Regulation (EU) 2016/679 (Apr. 27, 2016).

[35] Appendix A, Row 375 ("Section 999.313(a) has been modified to only require a business to disclose a general description of the business's verification process. A general description of the verification process would not raise any security or fraud concerns while still informing consumers' expectations regarding the response process.").

> ***request, a business shall be required to disclose a general description of its automated decisionmaking processes.***[36]

*   *   *

ESA appreciates the CPPA's consideration of these comments, and we look forward to continuing to work with the CPPA on these important issues.

Sincerely,

Gina Vetere

Gina Vetere
Senior Vice President and General Counsel
Entertainment Software Association

[36] This language aligns with the CCPA. Cal. Civ. Code § 1798.110(b) ("A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer."); Cal. Code Regs. Tit. 11, §§ 999.308(c)(1)(c), (2)(c) (requiring privacy policies to include the following information about deletion and access requests: a "[g]eneral description of the process the business will use to verify the consumer request, including any information the consumer must provide.").