December 6, 2019

Via Email

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

RE: <u>Written Comments on the Proposed CCPA Regulations</u>

To Whom It May Concern:

The Entertainment Software Association ("ESA")[1] submits these comments in response to the Attorney General's Notice of Proposed Rulemaking implementing the California Consumer Privacy Act ("CCPA" or "Act").[2] ESA's members share the Attorney General's goal of protecting the privacy and security of consumers' personal information, and we appreciate the significant efforts of the Attorney General's Office to provide industry guidance on the scope and application of the Act's requirements.

In particular, ESA appreciates the Attorney General's clarification that a business has the option of permanently and completely erasing, de-identifying, or aggregating personal information in response to a verifiable deletion request.[3] This proposed approach should be retained in the final regulation. Together with the cure period, these options serve as important

[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 900 video game companies in the State of California.

[2] California Department of Justice, Notice of Proposed Rulemaking Action (Oct. 11, 2019), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf.

[3] California Department of Justice, Proposed Text of Regulations, § 999.313(d)(2) [hereafter, "Proposed Regulations"]. As explained in the comments we filed in connection with the Attorney General's hearings on the CCPA, ESA requests that the Attorney General clarify that imprecise location information (such as zip code) is not "personal information" under the CCPA.

safety valves to protect consumers' rights while also avoiding "gotcha"-style enforcement and encouraging innovation in automated systems and processes to comply with consumer requests.

A number of areas remain, however, that create unnecessary uncertainty or require further clarification. Specifically, ESA requests that the Attorney General further revises its CCPA regulations to address the following issues:

- Explicitly permit businesses to protect the security and integrity of their systems and networks;
- Permit service providers to process personal information consistent with the statutory text;
- Delete the requirement to publish compliance metrics;
- Align the requirement to obtain explicit consent for privacy policy updates with the Federal Trade Commission's longstanding precedent for material retroactive changes;
- Clarify that providing a website address where a printable version of the privacy policy is available is sufficient to satisfy the requirement that the policy be printable;
- Clarify the requirements related to the opt out of "sale" by (a) specifying that personal information is not "sold" where it is not exchanged for "monetary or other valuable consideration"; (b) aligning the Proposed Regulations with the verifiable parental consent mechanisms recognized under the Children's Online Privacy Protection Act ("COPPA")[4]; (c) reducing the burden required for consumers who want to opt in; (d) eliminating the new requirement that businesses treat unverified deletion requests as requests to opt out; and (e) striking the new requirement that businesses pass through opt-out requests to third parties.

Each of these requests is considered in more detail below.

I. The regulations should explicitly recognize that businesses may take steps necessary to protect the security and integrity of their systems and networks.

As currently drafted, the CCPA's access, deletion, and portability rights[5] are vulnerable to abuse by malicious actors. Research involving similar consumer rights under the European Union's General Data Protection Regulation demonstrates how identity thieves, fraudsters, and other criminals can abuse such rights.[6] ESA and its members appreciate the Attorney General's recognition that measures to detect and prevent security incidents, fraud, and other unlawful

[4] 15 U.S.C. § 6501, *et seq.*

[5] As drafted, the Proposed Regulations do not appear to incorporate all of the statutory amendments that the California Governor signed into law in October 2019. For example, the statute, as amended, no longer requires all businesses to maintain a toll-free telephone number to receive consumer requests. ESA requests that the Attorney General harmonize the final regulations with all of the statutory amendments and apply the same methods for access, portability, and deletion requests.

[6] *See, e.g.*, Andrew Ross, "How Cyber Threats Could Grow Under GDPR," *Information Age* (May 14, 2018), *available at* https://www.information-age.com/cyber-threats-gdpr-123472491/; Martino et al., "Personal Information Leakage by Abusing the GDPR 'Right of Access,'" *available at* "https://marianodimartino.com/dimartino2019.pdf".

activity are important and permitted under the CCPA.[7] ESA's members urge the Attorney General to further clarify the scope of the regulations to further prevent malicious actors from abusing the CCPA rights.

Our members have implemented a number of important controls to help ensure that video game players have a fun and fair gameplay experience. For example, members may use proprietary technologies to determine when a player is using illegal software that infringes intellectual property, is attempting to engage in fraud in connection with in-game purchases, is harassing or bullying other players through an in-game chat, or is cheating or otherwise engaging in behavior that violates the game rules. Once this malicious activity is detected, an ESA member may take a range of actions including to suspend or block the account from using online game services or other action consistent with the game's terms of use. The malicious actor may then try to use the CCPA's access or portability rights to try to reverse engineer what specific information or action resulted in the suspension or termination of the account in order to try to circumvent the controls and evade detection in the future.

Moreover, individuals might try to use the portability right in ways that could violate a game publisher's trade secrets or intellectual property rights. For example, a person's raw gameplay and game character information may contain creative elements that cannot be technically transposed into another game or that could infringe the copyrights and other intellectual property rights that the game publisher has in such elements if ported to another game. The statutory text expressly directs the Attorney General to protect these rights and avoid having portability be used as a tool of infringement.[8]

The statutory text of the CCPA and the proposed regulations already appear to generally permit video game companies to deny consumer access, deletion, or portability requests where the company has a good faith belief that the request is fraudulent, malicious, or would facilitate unlawful activity. This would include rejecting requests for data sets that could be used to draw insights into system architecture (which could then be used to try to compromise those systems). However, to avoid any ambiguity and send a strong message to fraudsters and other bad actors that the state of California will not tolerate any abuse, we strongly urge the Attorney General to clarify the Proposed Regulations as follows:

> ***Nothing in the statute or these regulations shall restrict a business's ability to ensure security and integrity.***

In addition, the regulations should add a new definition of "security and integrity":

> ***"Security and integrity" means the ability: (1) of a network or an information system to detect security incidents that compromise the availability, authenticity, integrity, and***

[7] *See, e.g.*, Proposed Regulations, §§ 999.314(c) (permitting service providers to broadly use personal information for security and anti-fraud purposes), 999.315(h) (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). ESA requests that the Attorney General further clarify that the explanation that a business believes an opt-out request is fraudulent may be provided at a high enough level of generality to avoid making it easier for malicious actors to reverse-engineer or otherwise circumvent fraud detection mechanisms.

[8] Cal. Civ. Code § 1798.185(a)(3).

> ***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; (3) to protect trade secrets and intellectual property rights; and (4) to ensure the safety of natural persons.***

This revision not only furthers the purposes of the CCPA by taking into consideration security concerns and upholding legal rights (including those relating to trade secrets and intellectual property),[9] but also is consistent with clarifications recently sought by consumer advocates.[10]

II. The regulations should be clarified to avoid unduly restricting service providers' lawful data processing.

Section 999.314(c) of the Proposed Regulations states that a service provider cannot "use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity" unless it is "necessary to detect data security incidents, or protect against fraudulent or illegal activity."[11] The ISOR notes that this provision

> clarifies that a service provider's use of personal information collected from one business to provide services to another business would be outside the bounds of a "necessary and proportionate" use of personal information. Doing so would be advancing the "commercial purposes" of the service provider rather than the "business purpose" of the business.

ISOR at 22.

ESA and its members request that the Attorney General clarify this language to explain that service providers also can, consistent with the statutory text, use the information they receive from one business for the service provider's own operational purposes (including to provide services to other businesses) *as long as* the use is part of the services specified in the written contract with the business.

This clarification is necessary to avoid treating the statutory text in the "business purposes" definition as surplusage. The CCPA defines a "business purpose" to include the use of personal information for the "service provider's operational purposes."[12] In addition to detecting security incidents and protecting against fraudulent or illegal activity,[13] the statute expressly includes a number of other "operational purposes" that constitute "business purposes"

[9] Cal. Civ. Code §§ 1798.185(a)(3), (7).

[10] *See, e.g.*, Alastair Mactaggart, Letter to the Office of the Attorney General (Nov. 4, 2019) (regarding submission of amendments to the California Privacy Rights and Enforcement Act of 2020), https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

[11] Proposed Regulations, § 999.314.

[12] Cal. Civ. Code § 1798.140(d).

[13] Cal. Civ. Code § 1798.140(d)(2).

when performed by the service provider. These activities include (for example) providing analytic services, debugging to identify and repair errors, verifying customer information, and providing advertising or marketing services.

Importantly, these "business purpose" activities often require the service provider to combine and process personal information received from multiple businesses in order to provide the contracted-for services back to these businesses. For example, a mobile game developer may use a third-party debugging service that receives personal data (such as device and other unique identifiers) any time the game crashes. To effectively detect patterns (e.g., that a specific version of a mobile operating system is causing crashes on a specific type of device) and troubleshoot the problem, the debugging service may need to combine and analyze the information it receives from all of its business customers. If it is restricted to analyzing the data it receives from a single customer alone, it might not be able to detect the issue and the issue would remain unresolved. Similarly, an analytics service provider must combine and analyze the personal information that it receives from all of its business customers in order to derive the analytics reports and business insights that make up the contracted-for analytics services.

As drafted, Section 999.314(c) of the Proposed Regulations is ambiguous because it could be interpreted as prohibiting the service provider from combining and analyzing the information it receives from multiple business customers for these contracted-for business purposes. Such a reading would, in effect, convert all of the examples of "business purposes" contained in Section 1798.140(d) of the statute — except for the small subset of security and fraud purposes contained in Section 1798.140(d)(2) — into surplusage, which the California Supreme Court expressly disfavors.[14]

To avoid this result, the Attorney General should clarify that Section 999.314(c) of the CCPA regulations are not so narrow. Specifically, the Attorney General should specify that a service provider's data processing is "reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected" as long as the processing is to provide the services specified in the contract with the business.

This alternative interpretation resolves the relationship between the three definitions that the Attorney General considered in its ISOR (i.e., "service provider," "business purpose," and "commercial purpose") in a manner that is more consistent with the statutory text and avoids treating any statutory language as superfluous. Importantly, it aligns the "business purpose" definition with the language in the "service provider" definition prohibiting the service provider from "retaining, using, or disclosing the personal information for a commercial purpose *other than* providing the services specified in the contract with the business" or for "any purpose other than for the specific purpose of performing the services specified in the contract for the business."[15] It also tethers the permitted service provider activities to the context in which the service provider collects the information – i.e., to provide the contracted-for services (e.g., fraud

[14] *Copley Press, Inc. v. Superior Court*, 39 Cal. 4th 1272, 1286, 141 P.3d 288, 296 (2006).

[15] Cal. Civ. Code § 1798.140(v) (emphasis added).

detection, preventing security incidents, analytics, or debugging to identify and repair errors) to the business.

For these reasons, ESA requests that the Attorney General revise Section 999.314(c) as follows:

> A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity, except as ***reasonably necessary and proportionate to perform the services specified in the contract for the business***. ~~**A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary detect data security incidents, or protect against fraudulent or illegal activity**~~.

III. Publishing compliance metrics in a company's privacy policy does not further any statutory purpose and could create consumer confusion.

The Proposed Regulations impose certain reporting obligations on companies that alone or in combination, annually buy, receive for the business's commercial purposes, sell, or share for commercial purposes, the personal information of 4,000,000 or more consumers. Specifically, such businesses, must publish certain metrics regarding the number of requests they received, complied with, or denied, and the median number of days it took to respond to requests.[16] The ISOR explains that these metrics are necessary to inform the Attorney General, policymakers, academics, and members of the public about businesses' compliance with the CCPA.

However, this requirement serves no statutory purpose. Importantly, academics and members of the public do not need this information to ensure compliance with the CCPA, because the California legislature already refused to provide a private right of action in the context of consumer access, deletion, and opt-out requests.[17] The Proposed Regulations already require businesses to maintain a record of the requests they received and how they responded to those requests,[18] and the Attorney General has adequate means at his disposal to seek access to this information in the ordinary course of his regulatory and enforcement activities.

Moreover, the requested metrics do not achieve the stated purpose of assessing legal compliance. The fact that a request was denied does not, alone, demonstrate noncompliance, as the business might have lawfully relied on an applicable exception or lawfully denied the request based on a reasonable determination that it was fraudulent. Similarly, publishing the median number of days taken to respond to requests does not reflect on compliance. A business might report a median number of days lower than 45 days even if it had multiple occasions where it

[16] Proposed Regulations, § 999.317(g).

[17] SB 561 would have granted consumers a private right of action for any violation of the CCPA. SB 561 was placed on the suspense file earlier this year.

[18] Proposed Regulations, § 999.317(b).

unjustifiably responded *after* the statutory deadline had passed, and a business might report a median number of days higher than 45 days even if it had acted lawfully by properly seeking an extension under the statute.[19] Consequently, the requirement would appear on its face to be arbitrary and capricious.

Compiling the required metrics also might not be practically feasible. In many cases, a business will not be able to determine whether a consumer is a California resident, but may respond to the individual's request regardless as a voluntary best practice. The regulations do not appear to require these individuals to be considered when determining whether the 4 million threshold (which also has no reasonable basis and appears to have been arbitrarily selected) has been met, since "consumers" are defined to include only California residents. But this variability could significantly skew the metrics and make them less reliable.

Unfortunately, the most likely result of publishing these metrics is to create consumer confusion around their meaning and import.[20] In responding to consumer requests under the European Union General Data Protection Regulation, it is the experience of ESA members that each consumer request to exercise access or deletion of personal information is unique. However, a California consumer might compare his or her own experience against these metrics and become frustrated if their specific request is taking longer than the average or is denied, even though there may be entirely legitimate reasons for the delay or the denial. The consumer might also have the misimpression that these metrics represent legal standards, and that any delay or denial is unlawful, when this clearly is not the case for the reasons described above.

Consequently, we respectfully request that the Attorney General strike Section 999.317(g) of the Proposed Regulations and instead seek this information as needed in the ordinary course of regulatory and enforcement activities.

[19] The draft regulations require businesses to respond to requests to know and to delete personal information within 45 days, "regardless of time required to verify the request." Proposed Regulations, § 999.313(b). Forcing businesses to hurry through verification proceedures to meet arbitrary and capricious deadlines significantly jeopardizes the security of consumers' personal information and compliance with other laws that may require the business to withold the data from the consumer or to retain the data. *See, e.g,,* Cal. Civ. Code § 1798.81.5 (West). It also overlooks the statutory text in Section 1798.145(j)(1) that plainly states that a "time period for a business to respond to any verified consumer request may be extended by up to 90 ***additional*** days where necessary," such as where the consumer delayed the business's reasonable efforts to verify the request (emphasis added). To better protect consumers and faciliate legal compliance, we request that the Attorney General clarify that businesses can seek an additional 90-day extension where a consumer does not promptly verify their request.

[20] The requirement in the draft regulations that businesses disclose the value of the consumer's data and the results and methods of calculating that value also are likely to be impractical and encourage competitors to seek access to sensitive proprietary information. Proposed Regulations, § 999.307. In addition, this requirement runs contrary to established California case law that assigns no value to personal information. *See In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *14 (N.D. Cal. Sept. 20, 2011) ("Numerous courts have held that a plaintiff's 'personal information' does not constitute money or property under the [Unfair Competition Law]."). Accordingly, we propose striking sections 999.307(b)(5) and 999.337 of the Proposed Regulations.

IV. Any requirement to obtain explicit consent for privacy policy updates should align with longstanding Federal Trade Commission precedent.

Under the proposed regulations, a business must notify the consumer and obtain explicit consent before processing personal information for a purpose that was not previously disclosed to the consumer in the notice provided at or before collection.[21] ESA appreciates the Attorney General's concern that a "consumer could have reasonably relied on the information provided in the notice at collection when interacting with the business,"[22] and encourages the Attorney General to align the regulations with the more than fifteen years of Federal Trade Commission ("FTC") precedent on this issue.

The FTC has long held that *retroactive* application of *material* changes in a business's data practices may be deceptive or cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition.[23] In such circumstances, the FTC requires the business to provide prominent disclosures and obtain opt-in consent before using the consumer's data in a materially different manner than claimed when the data was obtained.[24]

This approach, which is based on whether the change is material (i.e., is likely to affect the consumer's conduct or decision with regard to a product or service[25]) and retroactive (i.e., applies to information collected prior to the effective date of the new policy), strikes the right balance of getting consumers the information they need and providing consumers appropriate choices, without unduly overwhelming consumers or interrupting the consumer experience when the changes have minimal impact on the consumer's privacy interests. As former FTC Chief Technologist Ashkan Soltani explained in his testimony before the California Senate Judiciary Committee's hearing on the CCPA, there is a significant risk that consumers will begin to get notice fatigue if they are asked to affirmatively assent to *every* new purpose for which a business processes data, regardless of whether that new purpose is materially different than those previously disclosed or is retroactive. In such circumstances, the Proposed Regulations could have the unintended effect of making consumers less likely to read notices before opting in to the changes.

To avoid this result, and to bring the CCPA into alignment with established legal precedent, ESA recommends that the Attorney General make the following changes in bold to Section 999.305(a)(3) of the Proposed Regulations:

[21] Proposed Regulations, § 999.305(a)(3).

[22] California Department of Justice, Initial Statement of Reasons, at 8-9, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf [hereafter, "ISOR"].

[23] Federal Trade Commission, Complaint, *In Re Gateway Learning Corp*., No. C-4120, 2004 WL 2618647, at 5 (F.T.C. Sept. 10, 2004), https://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917comp0423047.pdf.

[24] *Id.* at 3; *see also* Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change*, at 58, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[25] Federal Trade Commission, *FTC Policy Statement on Deception* (Oct. 14, 1983), appended to *Cliffdale Associates, Inc*., 103 F.T.C. 110, 174 (1984).

> ~~***A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection.***~~ *If the business intends to* ***retroactively*** *use a consumer's personal information for a purpose that* ~~***was not***~~ ***is materially different than what was*** *previously disclosed to the consumer in the notice at collection, the business shall* ~~*directly notify the consumer of*~~ ***prominently disclose*** *this new use* ***to the consumer*** *and obtain* ***express affirmative consent*** ~~*explicit consent from the consumer*~~ *to use it for this new purpose.*

V. The regulations should clarify that providing the website address for a printable version of the privacy policy is an acceptable way to enable print functionality.

Under the Proposed Regulations, businesses must make their privacy policies available in a printable format.[26] ESA and its members support the CCPA's goal of making privacy policies accessible for all consumers. As the "Internet of Everything" expands beyond desktop computers and laptops to include devices that have no reason to connect to a printer, ESA encourages the Attorney General to provide companies flexible alternatives to ensure consumers can access printable copies of privacy policies.

For example, video game consoles and handheld gaming devices do not have print functionality given that they are designed for gaming and entertainment purposes and not, for example, document processing. ESA's members take steps to ensure that consumers can access privacy notices through these devices and provide the website URL where a consumer can access a printable version of the privacy notice through a web browser on a printer-connected device. We believe providing the website URL qualifies as an "additional format" under the Proposed Regulations, but ask the Attorney General to clarify by revising the Proposed Regulations as follows:

> *Be available in an additional format that allows a consumer to print it out as a separate document****, such as a website address where the consumer can access a printable version of the privacy policy****.*

This approach is consistent with Section 999.306(c)(5) of the Proposed Regulations, which similarly permits businesses to include a website address for a business's privacy policies in the case of a printed form containing the notice of a right to opt-out.

VI. The Attorney General should clarify the "sale" opt-out requirements.

As explained further below, ESA requests that the Attorney General clarify the requirements related to the opt out of "sale" by (a) specifying that personal information is not "sold" where it is not exchanged for "monetary or other valuable consideration"; (b) aligning the Proposed Regulations with the verifiable parental consent mechanisms recognized under the Children's Online Privacy Protection Act ("COPPA")[27]; (c) reducing the burden required for consumers who want to opt in; (d) eliminating the new requirement that businesses treat

[26] Proposed Regulations, § 999.308(a)(2)(e).

[27] 15 U.S.C. sections 6501, *et seq.*

unverified deletion requests as requests to opt out; and (e) striking the new requirement that businesses pass through opt-out requests to third parties.

A. Specify that personal information is not "sold" if the exchange of data is not "for monetary or other valuable consideration."

ESA's members are focused on creating dynamic interactive experiences that challenge the boundaries of storytelling, competition, and social interaction. They are not in the business of selling data for commercial purposes or profit. Personal information often *does* need to be disclosed, however, between the operator of the gaming console or handheld device and the video game publisher in order to offer a wide range of video game services to players. In addition, ESA's members contract with a wide range of business partners who need personal information in order to provide important services that promote game development, enable game functionality, detect fraud and intellectual property infringement, and facilitate more effective promotion and advertising of game services to existing and prospective players. While some of these business partners are service providers, others may be considered third parties who use personal information to provide the contracted-for services but who do not receive such data for monetary or other valuable consideration.

Because there is significant confusion and uncertainty regarding the scope of the CCPA's "sale" definition, ESA requests that the Attorney General clarify that disclosures of personal information do not constitute a "sale" unless the personal information is disclosed "for monetary or other valuable consideration." This interpretation is supported by the plain text and legislative history of the statute, which require that personal information be exchanged for monetary or other valuable consideration.[28] An interpretation of the statute that treats *any* disclosure of personal information to another business or third party as a sale would impermissibly read the words "for monetary or other valuable consideration" out of the statute.[29]

Permitting disclosures of personal information to third parties who receive personal information to provide or facilitate video game services to players also is consistent with case law interpreting the meaning of "other valuable consideration." The Supreme Court of California has adopted the "bargained-for exchange" test for determining what constitutes

[28] Cal. Civ. Code § 1798.140(t); *see also* California Senate Judiciary Committee Bill Analysis (AB 375) at 17–18 (June 26, 2018) ("'Sell' as used in this bill would essentially delete this second section of the definition [contained in the preceding ballot initiative, which would have included] importantly the sharing of the information for no consideration to a third party for that party's commercial use. It is unclear why this change was made, but its effect would be that a consumer could not opt out of the sharing of their personal information with third parties, so long as there is not valuable consideration received."); California Assembly Floor Analysis (AB 375) at 7 (June 25, 2018) (referring to a "narrowing of the definition of 'sell' to remove reference to situations that do not involve valuable consideration").

[29] *Corley v. United States*, 556 U.S. 303, 314 (2009); *Smith v. Superior Court*, 137 P.3d 218, 221 (Cal. 2006) ("[W]e give significance to every word, phrase, sentence, and part of an act in pursuance of the legislative purpose.") (citing *People v. Canty*, 90 P.3d 1168, 1172 (Cal. 2004)) (internal quotation marks omitted); *Shoemaker v. Myers*, 801 P.2d 1054, 1067 (Cal. 1990) ("We do not presume that the Legislature performs idle acts, nor do we construe statutory provisions so as to render them superfluous.").

"valuable consideration."[30] In the typical scenario where personal information is disclosed to provide or facilitate video game services to players, the business promises to pay the third party money to induce or motivate the third party to perform the contracted-for services to players. In exchange, the third party promises to perform such services to induce or motivate the business to remit payment. Although personal information may need to be exchanged so that the third party can perform the contracted-for services, both parties have not "so understood and intended" the exchange of data to be the "plan and purpose for which the consideration was paid" or provided.[31] In such circumstances, personal information is not exchanged for "monetary or other valuable consideration" and, accordingly, there is no "sale" for CCPA purposes.[32]

B. *The parental consent mechanisms permitted under the regulations should align with the verifiable parental consent mechanisms recognized under COPPA.*

As drafted, Section 999.330(a) creates ambiguity regarding whether businesses can rely on existing processes for obtaining verifiable parental consent under COPPA to comply with the CCPA's parental consent requirements. Specifically, Section 999.330(a) states:

> A business that has actual knowledge that it collects or maintains the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501, *et seq*.

[30] *See, e.g., Jara v. Suprema Meats, Inc.*, 121 Cal. App. 4th 1238, 1248–49 (Cal. Ct. App. 2004) (explaining that "[t]o constitute consideration, a performance or a return promise must be bargained for… A performance or return promise is bargained for if it is sought by the promisor in exchange for his promise and is given by the promisee in exchange for that promise" (quoting Restmt. 2d of Contracts § 71)); *Stern v. Franks*, 35 Cal. App. 2d 676, 678 (Cal. Dist. Ct. App. 1939) ("Nothing is consideration that is not regarded as such by both parties" (quoting *Philpot v. Gruninger,* 81 U.S. 570, 577 (1871));; *People v. Cardas*, 137 Cal. App. Supp. 788, 791 (Cal. App. Dep't 1933 (although participants in a sweepstakes gave the promotor something of value, that gift was not a condition upon which the chance to participate in the sweepstakes was delivered; therefore, no consideration was exchanged); *see also Colorado Nat. Bank of Denver v. Bohm,* 286 F.2d 494, 496 *(9th Cir. 1961)* (In determining whether consideration was exchanged, the Ninth Circuit identified a fundamental common law principle "that consideration must be bargained for- it must be the thing which the parties agree shall be given in exchange for the promise").

[31] *People v. Gonzales*, 62 Cal. App. 2d 274, 282–283 (Cal. Dist. Ct. App. 1944) (quoting *State v. Danz,* 250 P. 37 (Wash. 1926)) (internal quotation marks omitted).

[32] ESA appreciates that, consistent with the statutory text of the CCPA, the draft regulations do _not_ require businesses to honor do-not-track signals as opt-out-of-sale requests. The draft regulations appear to appropriately recognize that "do not sell" is not equivalent to "do not track" by requiring businesses to honor user-enabled privacy controls only for _*sales*_ of personal information, rather than for online _*tracking*_. *Compare* Cal. Bus. Prof. Code Section 22575(b)(5) (defining "do not track" signals as communicating a consumer's "choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services"), *with* Proposed Regulations Section 999.315(c) and Cal. Civ. Code § 1798.140(t) (defining "sale" as the exchange of personal information "for monetary or other valuable consideration"). To avoid requiring technical compatibility with every "do not sell" plugin or setting that could emerge (which is not practically possible), ESA encourages the Attorney General to clarify in the final regulations that this requirement applies only to commonly-accepted and industry standard user-enabled privacy controls.

Section 999.330(a)(2) lists six specific methods that the Attorney General characterizes as "reasonably calculated to ensure that the person providing consent is the child's parent or guardian." However, it is not clear whether this list is exhaustive, and the list notably departs in some significant respects from FTC guidance.[33]

ESA requests that the Attorney General permit businesses to repurpose their existing verifiable parental consent processes under COPPA by, for example, expanding this process to include offline data that is sold for CCPA purposes. More specifically, the Attorney General should clarify the Proposed Regulations to align the permitted parental consent mechanisms under the CCPA with parental consent methods permitted under COPPA by making the following changes to Section 999.330(a):

> (1) A business that has actual knowledge that it ~~**collects or maintains**~~ ***sells*** the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. ~~**This affirmative authorization is in addition to any**~~ ***The business may utilize the same procedures used to obtain the*** verifiable parental consent required under the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501, *et seq.****; provided, however, that such consent is appropriately scoped to cover the sale of any personal information the business collects (whether online or offline)***.
>
> (2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include***, but are not limited to***:
>
> a. Providing a consent form to be signed by the parent or guardian ~~**under penalty of perjury**~~ and returned to the business by postal mail, facsimile, or electronic scan; . . .

C. Consumers should not be required to go through an unduly burdensome two-step process in order to exercise their opt-in choice.

Section 999.316(a) requires all consumers who wish to opt in to sales to undergo a two-step process through which they submit a request to opt in to the sale of personal information and then submit a subsequent confirmation of that request.

The CCPA was built on the recognition that "California consumers should be able to exercise control over their personal information." Requiring consumers to confirm their request to exercise a CCPA right detracts from that goal by introducing unnecessary steps that may unduly discourage the consumer from completing his or her request.

Additionally, the stated policy concerns underlying the two-step requirement for opt-in consent (including for minors between the ages of 13 and 16) are already addressed through the statute. The ISOR suggests that the new two-step requirement for opt-in requests is needed to

[33] For example, the first mechanism listed in the Proposed Regulations would require that a parent or legal guardian sign and return a consent form "under penalty of perjury," which is not required under COPPA. *Compare* Proposed Regulations, § 999.330(a)(2)(a), *with* 16 C.F.R. § 312.5(b)(i).

give "consumers the opportunity to correct an accidental choice to opt back into the sale of their personal information," and to provide "businesses additional assurance that the consumer has made a clear choice to exercise their right to opt-in." ISOR at 26. However, there is no evidence that opt-in requests are likely to be "accidental" and consumers, of course, retain the ability to opt out again at any time if their opt-in request was a mistake.[34] Requiring a double opt-in is especially disproportionate given that opt-out requests need not be verified. This discrepancy is likely only to confuse and frustrate the consumer.

Consequently, the double opt-in requirement should be removed from Section 999.316(a) and from the definition of "affirmative authorization" for consumers 13 years old and older. If the Attorney General rejects this request and retains the double opt-in requirement, then the regulations should at minimum similarly require the consumer to confirm his or her opt out request (i.e., double opt-out) before the business is required to comply with the request.

D. Requiring businesses to treat unverified deletion requests as opt-out requests diminishes consumer choice and creates practical challenges.

The Proposed Regulations introduce a new requirement that businesses must treat deletion requests that they cannot verify as requests to opt out of sales.[35] This requirement is not necessary to further any purpose of the CCPA. To the contrary, Section 999.313(d)(1) meaningfully *diminishes* the consumers' ability to control his or her own information.[36] The fact that a consumer chooses to submit only a deletion request and not also simultaneously opt out is significant, and is strong evidence that the consumer affirmatively chooses *not* to exercise the opt-out right.

Moreover, automatically converting the deletion request into an opt-out request does not provide the consumer any additional benefit. A business that denies the deletion request already must inform the consumer that the request is denied, at which point the consumer would be free to choose to submit a request to opt out of the sale of the information if she so desired.

Finally, this requirement may prove unworkable in practice. Consistent with the Proposed Regulations, a business may have one method for consumers to submit requests to delete data that requires a certain subset of the data the business maintains about the consumer, so the business can match the data provided with the particular requesting individual.[37] In contrast, the business may use a different mechanism for consumers to submit opt out of sales requests. If the two mechanisms used are different and collect different types of information (e.g., a webform request and user-enabled privacy settings), it might not be possible to convert the deletion request into an actionable opt-out request based on the data available to the business.

[34] Cal. Civ. Code § 1798.120.

[35] Proposed Regulations, § 999.313(d)(1).

[36] CCPA §§ 1798.105(b), 1798.120(b); Proposed Regulations §§ 999.306, 999.308.

[37] Proposed Regulations, § 999.323(b)(1).

For these reasons, ESA requests that the Attorney General strike Section 999.313(d)(1) from the final regulations.

E. Requiring businesses to pass through opt-out requests inadvertently would undermine consumer choice.

The Proposed Regulations require a business that receives an opt-out request not only to stop selling that consumer's personal information, but also to communicate that consumer's request to any third party to whom the business sold that consumer's data in the prior 90 days.[38] This new requirement does not advance any statutory purpose and, to the contrary, undermines consumers' ability to freely exercise control over their personal information.

This new requirement is unnecessary, because the statute already requires consumers to receive explicit notice before a third party may resell personal information.[39] This provision enables consumers to effectively exercise their opt out of sale rights with respect to the entire universe of parties who sell their data.

The new requirement also could have the unintended consequence of undermining the consumer's preferred choices. For example, a consumer may desire to terminate her relationship with video game publisher X, who may disclose personal information to third party Y to provide certain game services across a number of different video games. If the consumer continues to play a different game published by video game publisher Z, who also discloses the consumer's personal information to third party Y, then Y might be unable to continue to provide the game services when the consumer plays publisher Z's game title due to the opt-out request that it received in connection with publisher X's game. This might surprise and frustrate the consumer, who believed her opt-out request would apply only to publisher X.

In addition to creating consumer confusion, adding a new pass-through obligation for "sale" opt outs would be inconsistent with the statutory text and longstanding cannons of statutory interpretation. The CCPA contains a single pass-through obligation, requiring businesses to pass deletion requests on to service providers.[40] The California Supreme Court has held that "the expression of some things in a statute necessarily means the exclusion of other things not expressed."[41] Consequently, the inclusion of the deletion pass through means the exclusion of the pass-through requirement in the opt-out right must be given effect.

[38] Proposed Regulations, § 999.315(f).

[39] Section 999.305(d) of the Proposed Regulations requires companies that collect a consumer's data, but do not collect the data directly from the consumer, to (1) notify the consumer of that business's sale of their data, or (2) obtain a signed attestation from the source of the data that the source gave the consumer the relevant notice and obtain a copy of that notice. Both of these options are unlikely to be workable given the number of intermediaries that can be involved in a particular product or service offering. Instead, ESA encourages the Attorney General to permit the third party to obtain a broad confirmation by consumer type and contractual commitments that the source of the data has the right to share the personal information.

[40] Cal. Civ. Code § 1798.105(d).

[41] *Gikas v. Zolin*, 6 Cal. 4th 841, 852, 863 P.2d 745, 752 (1993).

For these reasons, ESA asks the Attorney General to remove Section 999.315(f) from the final regulations.

*　　　　*　　　　*

ESA appreciates the Attorney General’s consideration of these comments, and we hope to continue working with the Attorney General and his staff on these critically important issues.

Sincerely,

Gina Vetere

Gina Vetere
Senior Vice President & General Counsel
Entertainment Software Association