

Message

---

**From:** Lamb, Gerald [REDACTED]  
**Sent:** 11/19/2019 1:25:52 PM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** California Consumer Privacy Act

We have some questions and concerns regarding the applicability of the California Consumer Privacy Act. While it is clear that the Act is intended to protect all Californians and their constitutional right to privacy, the below definition for businesses that the Act applies to is not so clear. The definition "consumers" is applicable to California residents but we believe the Civil Code should be changed to help clarify it only pertains to such business related to California consumers.

Civil Code section 1798.140, subdivision (c) defines "business" as a for-profit business or other legal entity that collects and determines the use of consumers' personal information, and satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000) **in the state of California**; (B) Buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices **in the state of California**; or (C) Derives 50 percent or more of its annual revenues from selling consumers' (**consumer already defined as California resident**) personal information.

By doing so, it will help clarify which entities are necessarily effected by the Act. Our company is domiciled in another state but we do a small percentage of commerce in the state of California.

Thank you for your review and consideration.

Regards,  
Gerald Lamb  
MPP Co., Inc.

Message

---

**From:** Shawn Yadon [REDACTED]  
**Sent:** 11/22/2019 10:10:29 AM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** California Trucking Association Comments on the Proposed Regulations Concerning the CCPA  
**Attachments:** CTACommentsAGCCPA.PDF

To: Privacy Regulations Coordinator (Office of the California Attorney General),

On behalf of the California Trucking Association (CTA), attached please find comments pertaining to the proposed regulations concerning the California Consumer Privacy Act (CCPA).

Should you require any further information, please do not hesitate to let me know.

Kind regards,



**Shawn Yadon** | CEO  
California Trucking Association  
4148 East Commerce Way  
Sacramento, CA 95834  
[REDACTED]

W: [www.caltrux.org](http://www.caltrux.org)



---

We drive for a living. Safety is our priority.



November 14, 2019

Via Email to [PrivacyRegulations@doj.ca.gov](mailto:PrivacyRegulations@doj.ca.gov)

Privacy Regulations Coordinator  
California Office of the Attorney General  
300 South Spring Street, First Floor  
Los Angeles, California 90013

Re: CTA Comments on the Proposed Regulations concerning the CCPA

Dear Attorney General Becerra,

The California Trucking Association (CTA) appreciates the opportunity to submit comments to the California Attorney General as part of the Attorney General's rulemaking process under the California Consumer Privacy Act (CCPA). The California Trucking Association promotes leadership in the California trucking industry, advocates sound transportation policies to all levels of government, and works to maintain a safe, environmentally responsible and efficient California transportation goods movement system.

The CTA appreciates the common-sense approach the Attorney General's Office has taken in drafting its proposed regulations under the CCPA (the "Proposed Regulations"). For example, providing options for businesses to use to delete personal information when required ensures businesses have the flexibility to adopt protective mechanisms that fit each particular context. The clarity the Attorney General has brought to certain other issues is also welcome, such as the restrictions on disclosing certain categories of data, due to information security concerns, in response to right to know requests.

We appreciate the time, effort, and close attention the Attorney General's Office has devoted to crafting the Proposed Regulations, and its commitment to receiving comment from those who will comply with them. In this spirit, we respectfully submit our feedback regarding the current draft of the Proposed Regulations for your consideration on behalf of our members within the package transportation industry.



## **A. THE CCPA AND THE PACKAGE TRANSPORTATION INDUSTRY**

The CCPA will regulate package transportation providers as businesses operating in California that collect personal information relating to California consumers. For package transportation companies, certain unique CCPA issues arise from the fact that a significant portion of the personal information processed in core, day-to-day operations is received not directly from consumers, but instead from retailers and other corporate customers. This information takes the form of addressing details and package-related information, such as package dimensions and weight (collectively, “Shipping Information”).

For example, when a consumer buys a pair of shoes online, the online shoe retailer provides a package to a carrier along with associated Shipping Information. Consumers not only expect this information sharing, they in fact require it when they pay retailers and manufacturers to arrange for the shipping of products they have purchased.

The necessity of data sharing as a feature of daily package transportation operations raises several key questions under the CCPA. Our comments below relate to the issues we view as most critical:

1. Sharing Shipping Information with package transportation companies should not constitute a “sale” of personal information.
2. This is critical because a different finding would mean transportation providers receive Shipping Information only as “service providers” – a result that would be inconsistent with consumer expectations and would significantly impair the transportation industry, with no corresponding consumer benefit.

## **B. COMMENTS OF THE CTA ON THE PROPOSED REGULATIONS**

### **1. Sharing Data with Package Transportation Companies to Ship Packages Should Not be Deemed a “Sale” of Personal Information.**

The CTA respectfully submits that it is critical to the package transportation industry to confirm that retailers and other corporate customers do not “sell” Shipping Information when they provide that information to transportation providers. This clarification is critical, due to the scope of the definition of “sell” in the CCPA, because transportation providers inherently use Shipping Information for more than simply to deliver each individual package to each individual address. Shipping Information is inherently embedded into the operations of transportation providers, similar to how an organization might consume and integrate fuel or other supplies into its operations. For example:

- Carriers use Shipping Information continuously and on an automated basis for package routing within their networks; transportation and delivery planning and optimization; and to make decisions about package network optimization (including locations of facilities, retail outlets, staffing, “drop boxes” where consumers can pick up and leave packages, and capital investment). They do not simply use the information to deliver a specific package and then forget it.
- Shipping Information constitutes a combination of information received from customers, plus information carriers append from their own historical information and operations (including very specific details of package handling, status, and routing within a package network), and information they receive from third parties. The individual elements received from customers are integrated into this data and are not reasonably capable of being pulled back out.



- Carriers continuously and automatically update Shipping Information about individual packages with additional information concerning individual shipment attributes, and operational details and requirements for shipments meeting such attributes (e.g., handling of a particular package due to its dimensions and weight (“DimWeight”) or service level (e.g., standard vs. priority)) in order to fulfill deliveries and operate and improve the carrier’s package transportation network. Carriers do this in order to route large numbers of deliveries to the right place at the right time, to manage the transportation network, and to improve the shipping network for future deliveries.
- One of the more prominent examples of this is addresses: annually, carriers often correct tens or hundreds of millions of addresses that customers have submitted to them using information carriers collect while delivering packages, or from data acquired from, e.g., the US Postal Service. Once an address is corrected, it enables future shipments from any other corporate customer to reach that same address as desired by the consumer(s) resident at that address.

The use of Shipping Information by transportation providers beyond the simple delivery of each individual package to each individual address, when requested not by the individual consumer but by a retailer or other corporate customer, could therefore be considered to result in a sale of that information by the retailer to the carrier, but for the exception in Cal. Civ. Code § 1798.140(t)(2)(A).

- Subsection 1798.140(t)(2)(A) provides that a business does not “sell” personal information when consumers “direct the business to intentionally disclose personal information.” This is precisely what happens when consumers order goods from carriers’ corporate customers that need to be shipped.
- Specifically, when consumers buy products, they are directing retailers and other corporate customers to disclose Shipping Information to a transportation provider, instead of making their own separate arrangements with a transportation provider directly or, when applicable, directly picking up the merchandise from the corporate customer’s facility. In fact, consumers generally pay a separate and extra charge for shipping, arguably affirmatively obligating the corporate customer to share information with a transportation provider for shipping purposes.
- To exempt consumer-directed data disclosures from being a “sale,” the CCPA does not require that the consumer specify precisely who should receive their personal information. Instead, the § 1798.140(t)(2)(A) requires only that the consumer “direct” a retailer or manufacturer to “intentionally disclose” their information. Consumers who purchase merchandise from retailers or manufacturers have exactly this in mind – that their data will be provided to a carrier that will deliver the merchandise to them.

Shipping Information remains protected under the CCPA in the hands of the carrier. Carriers are businesses that determine the purposes and means of the processing of Shipping Information and must comply with the CCPA, including the various privacy obligations and protections established by the statute. This information is also protected by a longstanding federal law that regulates its handling and disclosure.<sup>1</sup>

The CTA believes the plain meaning of the CCPA establishes that retailers and other corporate customers transfer Shipping Information to transportation providers outside the definition of a “sale” pursuant to the direction of the consumer purchasing the product. But our members are seeing certain corporate customers interpret the law differently, positioning carriers as “service providers” as defined

---

<sup>1</sup> See 49 U.S.C. § 14908.



in the CCPA, out of a concern that disclosing data to a separate “business” carries a “sale” risk. This designation would prevent package transportation providers from being able to use Shipping Information for any purpose beyond delivering each individual package – a result that will impair operations across the industry with no corresponding consumer benefit. The CTA therefore respectfully requests the Attorney General to clarify the application of Section 1798.140(t)(2)(A) to Shipping Information that transportation providers receive from businesses, pursuant to the Attorney General’s rulemaking authority under Cal. Civ. Code § 1798.185(b)(2).

**2. Clarifying that the Sharing of Package Information Is not a “Sale” Is Critical to the Package Transportation Industry, because Deeming Transportation Providers as “Service Providers” Would Fundamentally Impair the Industry’s Ability to Operate, with no Corresponding Benefit to Consumers.**

A finding that transportation providers receive Shipping Information as “service providers,” and not pursuant to the direction of the consumer under Cal. Civ. Code § 1798.140(t)(2)(A), would fundamentally impair transportation industry operations and would be inconsistent with consumer expectations.

**a. Consumers Have Direct Relationships with Package Transportation Providers.**

When an individual consumer directly hires a carrier to ship a package, that carrier clearly acts as a business with respect to the consumer, not a service provider. The carrier thus has the corresponding obligations of a business under the CCPA, such as to accept and fulfill requests to know and requests to delete.

But if carriers are deemed to constitute service providers, and not businesses, when the shipper happens to be a corporate customer, then the carrier’s obligation will be to direct a consumer submitting a request back to the corporate customer. This is an inefficient result which would create a risk of consumer confusion. Indeed, our members’ experience is that consumers continue to see themselves as having direct relationships with the individual carriers delivering shipments to them, whether in connection with tracking shipment status, submitting claims, or requesting privacy-related information.

**b. A “Service Provider” Designation under the CCPA Will Create Fundamental Operational Issues for the Package Transportation Industry.**

The designation of transportation providers as “service providers” would also create a more fundamental problem. This is because, as we discuss in [Part 1](#) above, transportation providers inherently use Shipping Information received about an individual package for more than simply to deliver that package to the designated destination address. Shipping Information is inherently embedded into the operations of transportation providers and is therefore used for other transportation, planning, and operational purposes in the future.

While the CTA believes that the uses described in [Part 1](#) fall within the permitted uses for service providers under the statutory language in the CCPA, the Proposed Regulations would seem to preclude this finding.

- The CCPA permits corporate customers to share personal information with service providers for “business purposes” subject to appropriate contractual terms. The statute defines “business purposes” to include using personal information for a service provider’s “operational purposes, or other notified purposes, provided that the use of personal information shall be 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.” Cal. Civ. Code § 1798.140(d)

- The CTA believes that, if deemed service providers, carriers’ uses of Shipping Information would fall within this definition as “operational purposes, or other notified purposes” that have been notified via carriers’ consumer-facing privacy policies, and which are “reasonably necessary and proportionate . . . or . . . compatible with the context in which the personal information was collected [by the corporate customer].” *Id.*

Even if this interpretation is correct – which the CTA believes to be the case – we anticipate corporate customers may take a different position as a risk management measure because of concerns about other potential constructions of the law. The Proposed Regulations make this situation even more perilous for the industry.

**c. If Deemed a “Service Provider” Subject to the Restrictions in the Proposed Regulations, Package Transportation Providers Will Need to Disregard and Ultimately Discard Shipping Information about Each Individual Package after Delivery. This Result Would Impair Commerce and Harm Consumers, with no Corresponding Consumer Benefit.**

The draft text of § 999.314(c) within the Proposed Regulations published by the Attorney General’s Office would clarify that the right of service providers to use personal information received from customers is limited strictly to delivering the requested service. It states:

§ 999.314. Service Providers

- (c) 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. 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 to detect data security incidents, or protect against fraudulent or illegal activity.

As stated above, the CTA believes that package transportation providers are businesses, and not service providers, and that when retailers and other corporate customers share Shipping Information with carriers they do so at the direction of consumers pursuant to Cal. Civ. Code § 1798.140(t)(2)(A). But unless this is clarified through the Attorney General’s rulemaking process, we anticipate corporate customers will continue to insist on carriers accepting the designation as “service providers” under the CCPA. The current language of § 999.314(c), if adopted, would therefore preclude transportation providers from using Shipping Information for fundamental, inherent, and accepted purposes that do not create privacy risks for consumers.

- For example, if deemed a service provider, then once a carrier delivers a package, the carrier would not be able to use that delivery address (which in and of itself may qualify as personal information under the CCPA) or any details about the delivery (e.g., the precise location of a drop-off point) to facilitate the next delivery to that address. This is not in the consumer’s interest – as correct address information and details about the delivery point enable carriers to operate more efficiently, provide a higher level of service, and lower costs. And this finding would provide no consumer benefit. Carriers themselves are directly accountable to consumers under the CCPA.



- Carriers would also apparently be precluded from taking the position that accepted uses such as address correction are “proportionate” and “compatible” uses for a permitted “business purpose.” The CTA submits this would be an anomalous result that would not provide any consumer benefit.

Therefore, if the Attorney General declines to clarify the application of Cal. Civ. Code 1798.140(t)(2)(A) to Shipping Information processed by the package transportation industry, then the CTA would respectfully request the Attorney General to consider revising the Proposed Regulations to make clear, in the second sentence, that the use of Shipping Information by carriers to provide services to other customers – and indeed to others residing at the same address – and for other internal transportation operations-related purposes is permissible.

### **3. The Clarifications Requested by the CTA Are also Consistent with the law under the European Union General Data Protection Regulation, which Provides that Package Transportation Providers Are Controllers, not Processors, as to Shipping Information.**

The European Union General Data Protection Regulation (the GDPR) is arguably the most comprehensive and protective privacy law in the world. Even in the EU, under the GDPR, package transportation providers are deemed controllers that have the right to determine the purposes and means of the processing of Shipping Information.

- As the Attorney General’s Office will be aware, the definition of “controller” in the EU is analogous to the definition of “business” in the CCPA, in that both a controller and a business “determine[] the purposes and means” of the processing of personal information. Cal. Civ. Code § 1798.140(c)(1); GDPR Art. 4(7). The GDPR also contains the concept of a “data processor”, which, similar to a service provider under the CCPA, is defined as an entity that processes data on behalf of a controller. The controller/processor concepts have existed at the EU level since 1995, when the EU’s Data Protection Directive was passed, and they continue in effect under the GDPR.
- European regulators who have addressed the issue have consistently found that package transportation companies are best classified as “controllers,” not as “processors.” As an example, the United Kingdom’s Information Commissioner’s Office issued guidance in 2014 stating that a delivery service “will be a data controller in its own right in respect of any data it holds to arrange delivery or tracking ... such as individual senders’ and recipients’ names and addresses.”<sup>2</sup> More recently, the Bavarian Office for Data Protection Supervision issued 2018 guidance stating that “postal services for letter or package transportation” are generally “not data processing,” but instead “specialized services” offered by “an independent controller.”<sup>3</sup>

We respectfully suggest that the European practice reflects a recognition of the fundamental, inherent, and accepted purposes for which package transportation providers must use personal information to perform their daily operations at the level expected by both consumers and customers. We request the Attorney General to take a similar approach under the CCPA by clarifying the

<sup>2</sup> See Information Commissioner’s Officer, *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* at 12 (June 5, 2014), available at <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>.

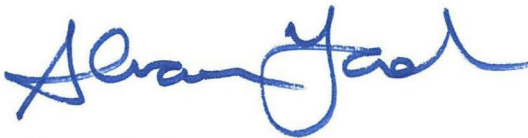
<sup>3</sup> See Bayerisches Landesamt für Datenschutzaufsicht [Bavarian Office for Data Protection Supervision], *FAQ zur DS-GVO: Auftragsverarbeitung, Abgrenzung* [GDPR FAQs: Data Processing, Distinguishing [between Controllers and Processors]] at 2 (July 20, 2018), available (in German) at [https://www.lida.bayern.de/media/FAQ\\_Abgrenzung\\_Auftragsverarbeitung.pdf](https://www.lida.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf).

application of Section 1798.140(t)(2)(A) to Shipping Information that transportation providers receive from businesses, pursuant to the Attorney General's rulemaking authority under Cal. Civ. Code § 1798.185(b)(2).

\* \* \* \* \*

We appreciate the Attorney General's review and consideration of our comments in this letter, and look forward to the Attorney General's continued efforts through the rulemaking process. For any questions or feedback, please contact me at [REDACTED]. We thank the Attorney General and his staff for the opportunity to provide our views for consideration, and look forward to working with you to address the matters outlined above.

With kind regards,



Shawn Yadon

CEO

California Trucking Association





SecureTheVillage

Turning People and Organizations  
Into Cyber Guardians

November 11, 2019

Attorney General Xavier Becerra  
Attorney General's Office  
California Department of Justice  
P.O. Box 944255  
Sacramento, CA 94244-2550

*Subject: CCPA and Minimum Reasonable Information Security Practices*

Dear Mr. Attorney General:

I write to you as the founder and President of a California nonprofit, *SecureTheVillage*. We are a community of information security practitioners; IT vendors and MSPs; attorneys with a practice in cyber; cyber-investigators; insurance and risk management professionals; law enforcement, including the FBI, Secret Service, and both the Los Angeles County and Orange County District Attorney's Office; and others. In addition to our base in Los Angeles, our community extends to Orange County and Sacramento.

I am writing in regard to the California Consumer Privacy Act (CCPA) *Right of Compensation* to consumers in the event of a data breach *except when the breached business maintains "reasonable security procedures and practices appropriate to the nature of the information being protected."*

As has been widely discussed, there is a great deal of uncertainty as to exactly what *"reasonable security procedures and practices"* is to mean.

In response to this uncertainty, *SecureTheVillage* has developed and published—as a free public service—a set of *Minimum Reasonable Information Security Management Practices*.<sup>1</sup>

For the reasons described below, we invite you to use our *Minimum Reasonable Information Security Management Practices* in assisting California establish appropriate reasonability requirements for organizations to follow in complying with CCPA and other information security management obligations.

---

<sup>1</sup> See <https://mrsp.securethevillage.org/>.



*SecureTheVillage* views these *minimum reasonable* practices as so basic to the responsibility of securing private consumer information that a failure to implement them should be considered *prima facie* evidence that an organization's information security procedures and practices are not reasonable. We developed them to be *commercially reasonable* and *reasonably achievable* for any company subject to CCPA.

It is important to note that we are not saying that an organization meeting these minimum practices has reasonable practices. To cite one example, the "reasonability" requirement for a large telecommunication or Internet Service Provider is considerably more than our suggested minimum. And even a company that meets our minimum standards might still not have reasonable standards appropriate to the nature of the information being protected. Our suggested minimum is designed to establish the floor, not set the bar.

*SecureTheVillage's Minimum Reasonable Information Security Management Practices* are based upon other existing information security standards. These include:

1. The NIST Cybersecurity Framework
2. International Standards Organization ISO 27001 family, Information Security Management
3. The Center for Internet Security's Critical Security Controls [CIS-20] (Identified by then Attorney General Kamala Harris in the California 2016 Data Breach Report)
4. New York State Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies
5. NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

*SecureTheVillage's Minimum Reasonable Information Security Management Practices* have nine basic elements.

1. Information Security Management
2. Information Security Subject Matter Expertise
3. Security Management of Sensitive and Private Information
4. Security Awareness Training / Culture Change (SecureTheHuman)
5. Security Management of the IT Interface
6. Security Management of the IT Infrastructure: Use of CIS-20 Critical Security Controls <sup>2</sup>

---

<sup>2</sup> At the present time, our incorporation of the CIS-20 is based upon the Center's Version 6 controls. We will be upgrading our minimum to the newer CIS Version 7 controls later this year or early in 2020.

7. Third-Party Security Assurance
8. Information Resilience
9. Information Security Governance

It would be my pleasure to meet with you and/or your staff to discuss how our *Minimum Reasonable Information Security Management Practices* supports California's need for a well-defined standard for *reasonable security practices*.

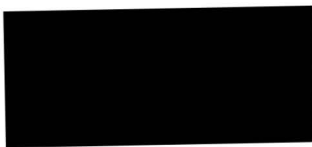
Thank you for your consideration. Thank you as well for your leadership in helping California find the right judicial answers to meet the challenges of cyber crime, cyber privacy and information security.

I look forward to hearing from you.

Sincerely,

A handwritten signature in blue ink that reads "Stan Stahl". The signature is fluid and cursive, with the first name "Stan" and last name "Stahl" clearly distinguishable.

Stan Stahl, Ph.D.  
*SecureTheVillage*  
Founder and President



Message

---

**From:** Yaakov Shapiro [REDACTED]  
**Sent:** 11/13/2019 7:16:35 AM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** comment on CCPA Propsed Text Regulations 999.312

Re 999.312 of CCPA Proposed Text Regulations:

There is ambiguity in the language of the following paragraph:

(a) A business shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, **and if the business operates a website, an interactive webform accessible through the business's website or mobile application.**

The word "or" in the phrase, "the business's website or mobile application" should be clarified. Currently, it can be interpreted in two ways:

- 1) If the business has a website and mobile application, both must have an interactive webform, or:
- 2) If the business operates a website, it is sufficient to have the webform either on the website or on the mobile application.

---

*Yaakov Shapiro*

[REDACTED]

[REDACTED]



Message

---

**From:** Brian Pier [REDACTED]  
**Sent:** 11/18/2019 6:40:23 AM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** Comment on the CCPA

I have a concern regarding the proposed regulations associated with the California Consumers Privacy Act (CCPA).

Section 999.326 permits an authorized agent to submit a Request to Know and/or a Request to Delete (Requests) on behalf of a consumer. I foresee businesses who will offer to conduct these requests for consumers for a fee. These businesses may collect contact information about a large number of organizations who maintain data about California Consumers - pretty much any business in California who meets the income standard - and will submit the Requests to all of these organizations, even though many of the organizations will have no information about the consumer. Technology easily support submitting the requests to thousands of organizations with little effort.

There would a significant amount of work involved in responding to these request, even if almost every response is "We have no information about the consumer". Just the process of validating these requests would be a significant burden. The proposed regulations certainly favor the professional authorized agents over the companies complying with the CCPA.

I work for a company that has data that will be governed by CCPA. We never sell information about individuals. We only have information about customers, employees and employment candidates.

Please implement the regulations in a manner that prevents us from receiving a large number of inquiries from authorized agents regarding individuals for whom we have no information. I can foresee this becoming a significant burden that only generates revenue for a professional "authorized agent".

While various modifications to the regulations could be incorporated to accomplish this request, could you limit the authorized agent requests to companies who sell information to others? Conversely, you could exempt organizations who do not sell information (as stated in their privacy policy) from requests from authorized agents.

For those of us who do not sell any personal information, we should not be subjected to a burdensome deluge of requests from authorized agents. For us, our customers, employees and job applicants supplied the information to us so they already know what information we have about them. We have no other sources of information about individuals beyond the individual themselves. While we know we may need to respond to other individuals who submit Requests, I fear what professional authorized agents could create significant work for companies in similar situations.

Regards,  
Brian Pier  
[REDACTED]

Message

**From:** [REDACTED]  
**Sent:** 11/3/2019 8:48:56 PM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** Comment regarding CCPA and its associated regulations

[REDACTED]

\*\*\*\*\*  
\*\*\*\*\*

Judging by this poorly conceived statute, the foolish proposed regulations, and AG Becerra's public statements, I can only assume that the Attorney General and the Legislature are determined to victimize small businesses and sole proprietors like me and drive us out of California forever.

First, neither the proposed regulations nor the various amendments that have passed or been put forward in the Legislature have addressed a fundamental ignorance underlying the law: the thresholds of applicability. Judging by the first statutory stipulation -- gross revenues of \$25 million a year or more -- one may presume that the legislatures who drafted the CCPA intended it to apply mostly to large and medium-sized corporations. (My total income from all sources throughout my entire life has never even approached that figure.) However, the stipulation that it applies to any business that collects personal information on 50,000 or more households per year betrays the technical ignorance of the Legislature and, in failing to usefully clarify it, the OAG. Because the statute defines "personal information" so overreachingly broadly, the law likely applies to nearly everyone on the Internet, including individuals with personal blogs or even social media accounts; it could easily be interpreted to apply to any person whose Twitter feed receives more than 137 individual impressions a day, even if none of those impression are from California residents! This is patently absurd and seems at odds with the implied statutory intent.

In this way, the CCPA, and the proposed regulations, treat sole proprietors like me in exactly the same manner as tech giants like Facebook or Google, presuming vast legal, technical, and service resources that I simply do not possess and am by no reasonable standard able to afford.

For one, it presumes that I possess contractual leverage over billion-dollar tech companies. For example, the law expects that if my website uses the Google Fonts service, or posts an embedded YouTube video, I should be able to contractually dictate Google's data practices, which companies like Google have no intention of or financial incentive to permit. I can assure you that no one at Google would ever even respond to a call or email from small fry like me, much less consider amending their standard terms of service.

The CCPA also exposes small businesses and sole proprietors me to significant legal liability for simply using modern devices, software, or tools such as cloud-based data storage or content delivery networks (CDNs). The normal use of any iPhone or Android mobile device and those devices' associated apps and services may collect significant amounts of what the law defines as personal information about literally anyone I interact with or even walk past. Any Windows 10 or iOS device is laden with telemetry and data mining tools, some of which cannot be turned off without software changes that violate the license terms. To mitigate that data gathering to any meaningful degree requires advanced technical knowledge and/or specialized tools, and even that cannot stop the full range data collection and sharing that CCPA and the proposed regulations seek to control. Simply loading contacts onto my phone or scanning my incoming email with an antivirus program that uses cloud services therefore becomes a potentially forbidden disclosure.

The law further presumes that all businesses engage in the type of data aggregation and consumer profiling that have made Facebook and Google the subject of well-deserved public criticism. For example, the law and proposed regulations not only assume, but INSIST that I be able to identify an individual consumer across different devices and types of engagement -- that I associate the face of an individual in the background of a photograph I published as part of an article with IP addresses in a server log and an email address in a newsletter signup list. For those of us who are not

data-mining tech giants, that is neither feasible nor particularly desirable. I usually have very little legitimate business interest in connecting such dots, and my doing so would be of no benefit to my website visitors or clients. As a consumer, I do not like being the subject of such data mining and routinely take steps to limit and thwart such “big data” aggregation. And yet, the State of California wishes to mandate that aggregation and correlation in ways that seem contrary to the interests of consumers as well as businesses operating in good faith.

Consequently, the mandatory timeframes proposed for response to requests are frighteningly daunting. I am a sole proprietor, and I do not routinely aggregate different types of consumer data unless I have some pressing reason to do so. To respond to the extent the law and proposed regulations require to even a single access request would take me days of work. And yet, AG Becerra not only thinks I should be able to respond to an unlimited volume of requests from different individuals in a month and a half, but has also expressed his wish that I and my business should be subject to personal civil actions for failing to do so. Does he insist that I also be able to juggle plates while standing on my head?

Furthermore, the opt-out request rules are, for all intents and purposes, technologically impossible to fulfill to the letter of the law and proposed regulations. For example, if I process an opt-out request from a particular consumer and they then access my websites or services from a device unknown to me, or via a proxy or VPN, their data may again be collected by advertisers or provided automatically to other service providers in ways that the extremely broad definitions specified in the statute would deem to be for commercial purposes. Again, this requires no bad faith or deliberate action at all -- any website with Google Ads may run afoul of these rules for this reason, even if the website’s owner has taken reasonable, good faith steps to comply with the opt-out request.

(As with the GDPR, the law’s presumption that an IP address is personal information rests on extremely dubious technical grounds. While IP addresses can sometimes indicate an approximate geographical location, an IP address by itself can only rarely identify a specific individual, and can generally only do so in combination with other information. For example, many Internet service providers use dynamic IP addresses or IP address pools, where any customer with an active connection may be arbitrarily assigned an available IP address from the pool; if I turn off my modem for longer than about 30 minutes, my IP address will likely be different when I reconnect. Furthermore, a substantial number of consumers use proxy or VPN services that hide the consumer’s actual IP address from any visited sites or services. Absent some other correlation information, there is no reason to assume that the actual human user associated with a specific IP address recorded in a log is even in the same country indicated by the IP address, and a single user using a proxy or VPN service may be able to visit the same website or service repeatedly from different endpoint IP addresses. This is an area where sensible regulation could clarify that IP addresses are only deemed personal information if they can reasonably be used to identify a specific individual or household, which is by no means always the case.)

As a freelance writer, the implications of the CCPA for my free speech rights and my professional livelihood are extremely worrisome. The statute exempts from deletion requests information necessary to exercise my free speech rights (or so it says), but if I submit an article containing literally any identifiable information about any living Californian for publication in any manner that benefits me economically, any person mentioned (even public figures) can prohibit that publication by filing an opt-out request -- and, if AG Becerra has his way, personally sue me if I fail to do so, in a way that seems contrary to the intent of California’s anti-SLAPP laws. This again is absurd and, despite whatever token mention has been made of preserving free speech and the public interest, represents a significant potential chilling effect and threat to the exercise of First Amendment rights.

As a consumer, I’m annoyed that no provision has been made for me to selectively opt out of disclosures or request selective deletion, which forces businesses and online services into an all-or-nothing approach that will ultimately leave consumers with fewer options and less control over the use of our data. This is hardly a desirable outcome.

My question about this law is “Cui bono?” It is onerous for most businesses other than Facebook, Google, Apple, Microsoft, etc. (which will likely test the limits of any available loophole, since fines for them are part of the cost of doing business). It encourages and mandates data aggregation in a way that seems directly contrary to the protection of consumers’ privacy, and it’ll bring yet another new load of confusing legalese and notification banners that most consumers will never read. It will impose new burdens on the courts and the OAG to investigate and/or try complaints.



It's hard to see any substantive benefit to privacy, and the price tag for what is at best a modest moral victory will be extremely high.

I recognize that the OAG is not in a position to change the statutory language of the law and its amendments -- a task that, to the dismay of most observers, must be left to the fools in Sacramento who contrived this legislation in the first place. However, if AG Becerra would temper his determination to punish businesses and businesspeople, reevaluate his assumption businesses of any size all have the resources and the bad faith of Facebook, and consider the devastating financial impact this law will have on the state's economy, he COULD direct the OAG to provide common-sense clarifications of the law's many confusing ambiguities and contradictions and at least blunt the edge of the knife the CCPA is sticking between my ribs.

\*\*\*\*\*  
\*\*\*\*\*

---



Message

**From:** [REDACTED]  
**Sent:** 11/19/2019 4:50:51 PM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** Comment regarding CCPA and its associated regulations

\*\*\*\*\*  
\*\*\*\*\*

The proposed regulations would not require any type of verification for opt-out requests. This is a foolish choice that will lend itself to endless abuse, directed not only at businesses attempting to act in good faith, but also against individual consumers.

With no verification requirement, it would be very easy for malicious individuals or their automated "bots" to submit bogus opt-out requests on behalf of any number of legitimate customers or users (e.g., those who have posted comments or reviews in connection with a purchase). Businesses would have little choice but to respond to most or all of those bogus requests, since the regulation would effectively prohibit them from conducting the type of verification the other proposed rules require -- and failing to respond to a request (or indeed even responding to say the request appears to be fraudulent, even if it's obviously spam) would carry heavy potential legal liability.

In this way, pranksters or other perpetrators of online abuse could send businesses chasing their own tails trying to respond to every fraudulent opt-out request, or sign other legitimate customers out of services that customer wants and has expressly requested. For example, if a consumer has asked to receive email updates on sales or special offers, a third party could, without the consumer's knowledge or desire, sign the consumer out of such updates by submitting an opt-out request in the consumer's name.

That is manifestly ridiculous, particularly given the technical difficulties involved in complying with the opt-out requests. Again, it lends itself to abuse, particularly where businesses have provided their consumers options to make a request electronically. Any online form is a constant target for spam and malicious activity, and the way this rule has been framed would essentially require all businesses to play along with spam bots, hackers, and other malicious entities, to the detriment of privacy and security.

I gather that OAG wants to make sure there is not an undue barrier to consumers exercising their opt-out rights, but I see no sensible reason that opt-out requests should not be subject to the "reasonable degree of certainty" verification standard described elsewhere in the proposed rules. Doing so would be common sense and a bulwark against the abuse the no-verification rule invites.

\*\*\*\*\*  
\*\*\*\*\*

Message

---

**From:** Webb Howell [REDACTED]  
**Sent:** 11/21/2019 8:33:14 AM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** Comment

I would like to see the rule include a definition of "Consumer." I would like to know if "consumer" includes business-to-business relationships and data gathering, as most businesses do for the purpose of sales and marketing.

Thank you.

Webb Howell



Message

---

**From:** Chris Pedigo [REDACTED]  
**Sent:** 11/7/2019 5:56:59 PM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** DCN Comments re CCPA  
**Attachments:** DCN letter to CA AG 2019-11-07.pdf

Hi – I am submitting [these comments](#) regarding the proposed regulations for the enforcement of the California Consumer Privacy Act (CCPA). I have also attached the comments as a pdf. Please let me know if you have any questions or if I should submit these comments in a different format.

--

Chris Pedigo  
SVP, Government Affairs  
Digital Content Next  
[REDACTED]  
[REDACTED]

Follow us on Twitter: [@DCNorg](#)  
[Sign up](#) for our weekly newsletter, InContext, for insights in digital media.



November 7, 2019

Privacy Regulations Coordinator  
California Office of the Attorney General  
300 South Spring Street, First Floor  
Los Angeles, CA 90013

RE: California Consumer Privacy Act Regulations

Dear Attorney General,

We appreciate the opportunity to comment on the regulations proposed by your office to implement the California Consumer Privacy Act (CCPA). Founded in 2001 as the Online Publishers Association, Digital Content Next (DCN) is the only trade organization in the U.S. dedicated to serving the unique and diverse needs of high-quality digital content companies which enjoy trusted, direct relationships with consumers and marketers. DCN's members are some of the most trusted and well-respected media brands that, together, have an audience of 256,277,000 unique visitors or 100 percent reach of the U.S. online population<sup>1</sup>. In layman's terms, every person in the U.S. who goes online will visit one of our member companies' websites at least one time each month.

We intend to submit detailed comments with specific questions and concerns about the proposed regulations by the December 6 deadline. In the intervening time, however, we feel compelled to draw your attention to the possible interplay of privacy regulation and market dominance, based on our experience complying with the General Data Protection Regulation (GDPR) in Europe. Legislation is often written with the assumption that businesses are free to negotiate the terms under which they integrate with their suppliers but, as detailed in the open letter to Google CEO Sundar Pichai<sup>2</sup> that we penned in April 2018 alongside three other publisher trade associations, that is not always the case. In Europe, Google opted for an implementation of GDPR compliance that favored their interests while going against those of both publishers and consumers. We hope to preemptively avoid this happening again out of respect for consumers who are visiting our sites and apps.

Based on the legislative text of the CCPA and the proposed regulations issued by your office, when a consumer exercises their Do Not Sell right, publishers may not sell a consumer's data but would be allowed to collect and use it for business purposes (CCPA Sec 1798.140 (d)). In

---

<sup>1</sup> *comScore Media Metrix Multiplatform Custom Audience Duplication*, December 2017 U.S.

<sup>2</sup> [Open letter to Google CEO Sundar Pichai](#), signed by Digital Content Next, the European Publishers Council, the News Media Alliance, and the News Media Association.

addition, any company acting as a third party on a publisher's website may not collect and use a consumer's data except for a business purpose on behalf of the publisher. Service providers may still assist publishers in delivering their service but only on behalf of the publisher and are prohibited by contract from using the data for any other purpose. This is in line with consumer expectations as the data is being collected and used within a single context.

Where a third-party company is not a service provider to the publisher, however, they must cease using the consumer's data for secondary purposes. For example, companies such as Facebook via the "like" button and Google via their ad technology services would be third parties unless and until the consumer directly interacts with those services by clicking on the "like" button or the ad. Similarly, in the case of Google's Accelerated Mobile Pages (AMP), where Google is providing a service to publishers by hosting the content on their server, the consumer has no intention of interacting with Google. Indeed, most consumers would have no knowledge that Google is involved in helping serve the content. In these examples, as third parties, Facebook and Google must cease the collection and use of a consumer's data except for security and fraud purposes or for business purposes strictly on behalf of the first party as detailed in Sec 1798.140 (d) of the CCPA. These third-party companies must not add data about the consumer to any profile that may be used to tailor advertising to that consumer on a different, unrelated website.


We are concerned that, similar to what happened with the GDPR, some third-party companies will attempt to avail themselves of creative implementations of compliance with the CCPA such as for instance declaring themselves to be a business or an agent of the first-party business with which the user is interacting — in clear defiance of consumer expectations — or by attempting to burden publishers with unreasonable compliance requirements on their behalf (such as their compliance with section 115(d) of the CCPA). Because of a market structure that is heavily dominated by a small number of companies providing services essential to publishing, publishers may not have enough market leverage to negotiate with these third parties to obtain sensible contractual terms that align with the reasonable expectations of consumers who are visiting our sites and apps.

We are grateful for the opportunity to comment on the proposed regulations issued by your office and will provide more detailed comments in the coming weeks. In the meantime, please do not hesitate to contact us with any questions.

Sincerely,



Jason Kint  
CEO  
Digital Content Next



Chris Pedigo  
SVP, Government Affairs  
Digital Content Next



## Meeting with Roger McNamee on October 28, 2019, memorialized October 28 and 31, 2019

- Four problems: democracy, public health, privacy, competition
  - Antitrust law deals with the last
  - All start from surveillance capitalism (Shoshana Zuboff's book)
- Need to assert personal data as a human right rather than as an asset
  - The assertion that you own data if you touch it is problematic
  - Risks of data portability are high: need informed consent from everyone touched and need to offset the asymmetry that favors incumbent players (Facebook will profit from data portability)
  - Corporations have data that they touch and data they acquire; they will sell everything: Banks, health records (prescription data), menstrual cycle data becomes Facebook's property
  - What would consumer protection look like if data is a human right? Not "own your data," but accountability for social costs, like bans on cloning or private nuclear research
  - Not a First Amendment issue because it's not about who posts but who gets amplified. Algorithms encourage speech that leads to fight-or-flight responses
    - Going after data can solve problems with democracy and public health
  - No "Occam's Razor" solution better than this: aim for solution where data cannot be used to harm you; it's not an asset but off-limits.
- Need CCPA regulations to be as close to the endpoint as the law will allow.
  - GDPR was an almost perfect response based on knowledge of the problem as understood 3-4 years ago. CCPA can fix what was missed.
  - First problem: Thought the problem was data transfer on individual sites, not the overall marketplace. Restriction on a particular site only addresses a subset of data. Only 0.1-1% of data at Google, Facebook, Amazon, Microsoft is directly collected. Most is from tracking or is bought.
    - Fix by looking at data minimization/ When providing a service, there should be limits on what data can be used. Not OK for any site to have all health, banking, location records.
    - Must protect the consumer by recognizing that marketing has shifted: companies have all the data from all the people. From life events they determine common patterns and forecast. Need high-quality data.
    - They also control access to information and only offer what serves them.
    - The problem is that the marketer has nearly perfect information and the consumer has only what the platform allows (surveillance capitalism = authoritarianism)
    - Solution: in perfect world (1) only the first party could use the data. Uber can use location and phone number for one ride only. Uber would have to change prices and make explicit the true cost of the ride. (2) the use of data "voodoo dolls" would be banned; can't use existing data. Compare the chemical industry in the 1950s. Society changed and made the companies internalize the externality of pollution. Need to make companies internalize the costs of undermining democracy

- First step is to allow litigation. Worth it to try and include a right of action in the regulations and lose. Some actions have a cost.
- Second problem (easy one): GDPR allowed platforms to create their own dialog boxes; companies used eye tracking and dark patterns to manipulate and 95% of Europeans did not take advantage of protections.
  - Need a factually accurate dialog box “this company knows everything about you and their economic model is to control your choices.”
  - It’s a flaw with CCPA if it can’t do this.
  - CCPA allows automatic opt-out: What about a tweet that “I opt out of all data sale”?
  - But a setting on a phone may work.
  - The biggest problem is companies you don’t interact with: credit card processors and health care data companies. Can they use the data if they launder it?
  - Why not a lifetime lookback instead of 90 days? I’d make this an official comment. Data doesn’t get old this quickly. 91-day old data is still fresh.
  - What about sale vs. transfer? The big scary people (Google, Microsoft, Amazon, Facebook) complemented by wannabes: traditional data brokers, data marketers like credit card companies (MasterCard worse than Visa)
- Current corporations are flexible and morph around regulations (unlike corporations with assets like factories). They argue against them until they’ve changed their business models.
  - Amazon does microtargeting, but can just earn money from retail.
  - Very easy to circumvent regulations; surveillance capitalism is inherently dangerous
  - Facebook is “swapping” not selling, and maybe stopped in 2015 when it got caught. But 2010-2014 allowed 9 million apps to have access to friend lists. Swaps with hardware platforms (Xbox, PlayStation, Apple? Android?) Everyone on Facebook was affected.
  - CCPA can take the conversation to a level where it needs to go. DOJ should share something it can do and give a list of things it can’t solve yet under current law(e.g. SB 561)
  - Use CCPA regulations to leave California better off than today



November 6, 2019

The Honorable Xavier Becerra  
California Department of Justice  
Office of the Attorney General  
1300 I Street  
Sacramento, CA 95814

Dear Attorney General Becerra:

I enjoyed speaking with you at the Platinum Advisors client retreat in Sonoma recently, and sharing with you the prominent role the video game industry plays in California's entertainment and technology sectors. During our conversation, I mentioned our industry's interest in the California Consumer Privacy Act (CCPA) Rulemaking. I wanted to follow up on that matter, briefly.

We appreciate the important work of your office in providing much-needed regulatory guidance regarding the application of the CCPA. For the video game industry, the most critical issue is ensuring that there are reasonable means to address the security and integrity of online games and game networks. Specifically, our members who publish video games are asking for explicit confirmation that the CCPA does not prevent them from protecting players of online video games from harassment, malicious conduct, and cheating by other players and from detecting and preventing cyber intrusions, the theft of services and infringement of intellectual property related to the game. We believe that the text of the CCPA supports this interpretation, but we ask that the regulations leave no doubt.

When tens of thousands—or, in some cases, millions—of players meet up in online worlds to adventure together in competitive games, it is an unfortunate reality that some individuals may seek to harass, cheat or otherwise make the game less enjoyable for other players or try to gain unauthorized access to game content and features. Game publishers invest significant resources to root out and address this activity to help ensure that all players have a fun gameplay experience. These measures may include:

- employing customer support staff to review reports of abuse,
- moderating chat consistent with game terms of service and privacy policies,
- deploying technologies to detect cheating, fraud, grooming, and other harmful behavior, and
- imposing escalating measures to enforce the game rules or codes of conduct and combat unlawful activity including, in some cases, suspending, blocking, or banning players and deleting their accounts.

If a game gets a bad reputation because of pervasive cheating or harassment, some players may leave the game and new players may be discouraged from joining. Therefore, publishers invest significant resources in protecting players from potential cheating, harassment, and other harmful activities.

Data privacy laws directly impact publishers' efforts to discourage, detect and protect against harassment, cheating, and other malicious conduct. For example, a game publisher may need to collect and retain personal information—such as screen names, IP addresses, and device IDs—along with



gameplay data, for purposes of detecting anomalous behavior and identifying which particular individual is engaged in fraud, cheating, or other harmful activities.

If data privacy laws do not clearly allow publishers to continue engaging in these activities, some individuals may try to use these laws to undermine these important player protections. For example, in other jurisdictions that already have a data access right, our members have experienced some individuals abusing that access right to try to learn more about what triggered the game publishers' security, cheat, or fraud detection systems (e.g., common IP addresses across multiple fraudulent accounts) for purposes of evading them in the future.

We recognize, of course, that most consumers will not abuse the access right in this manner. To be clear, we are supportive of the CCPA's access right, and members who operate in jurisdictions that have access rights already provide players access to personal information as legally required. But it is important that the CCPA's access, deletion, and other consumer rights are reasonably qualified to ensure that bad actors cannot misuse the CCPA to conduct forensic data analysis related to security, cheat, fraud and other systems for purposes of identifying weaknesses, avoiding future detection, and engaging in further fraud or other harmful activities.

In addition, some individuals may seek to bypass the game's security features, steal services from game networks and/or infringe the game's intellectual property, to the detriment of the publisher and often other players as well. For example, in a subscription-based massively multiplayer online game, fraudsters may steal valid account credentials from a player or use stolen credit card information to create a game account, which they then build up and sell on secondary markets (i.e., through extensive gameplay by an expert player, they "level up" the account so that it is quite powerful and then sell the game account for real money on an unauthorized third-party site). This conduct violates the publisher's terms of service, results in fraudulent account charges, and frustrates other players whose game characters are not as powerful because they followed the game rules and played the game as intended. The publisher also is harmed if it later refunds the unauthorized charges once it detects the illegal activity. The CCPA regulations should explicitly balance privacy rights with these important consumer protection and intellectual property-related concerns.

We look forward to working with you and your staff on these important issues, and we will be submitting more extensive comments in the Rulemaking, including suggested redline language on this issue and other matters, in December. Thank you for your consideration.

Sincerely

A handwritten signature in blue ink, appearing to read 'TFoulkes', with a long horizontal flourish extending to the right.

Thomas Foulkes  
Vice President, State Government Affairs  
Entertainment Software Association

Message

---

**From:** James Harrison [REDACTED]  
**Sent:** 11/19/2019 2:56:05 PM  
**To:** Privacy Regulations [PrivacyRegulations@doj.ca.gov]  
**Subject:** Regulatory Impact Assessment of CCPA  
**Attachments:** 00395287.pdf

On behalf of Californians for Consumer Privacy, we respectfully submit the attached comments regarding the Standardized Regulatory Impact Assessment prepared on behalf the Attorney General. If you have any questions regarding CCP's comments, please contact me.

Thank you.

James Harrison

---

James C. Harrison  
Remcho, Johansen & Purcell, LLP  
1901 Harrison Street, Suite 1550  
Oakland, CA 94612  
Office: 510-346-6200

[REDACTED]  
[www.rjp.com](http://www.rjp.com)

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication



November 19, 2019

The Honorable Xavier Becerra  
Attorney General  
1300 I Street, Suite 125  
P.O. Box 944255  
Sacramento, CA 94244-2550

Dear Attorney General Becerra:

We write to with respect to the Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 (“CCPA”) Regulations, prepared in August 2019 by Berkeley Economic Advising and Research, LLC.

We have multiple questions with respect to the assumptions used, erroneous facts included, and conclusions reached. We believe it vastly overstates the economic impact of CCPA, as a result of guesses made by the authors, as opposed to sound business assumptions.

We set forth below our comments and requests for additional information.

**In preview, we conclude:**

- 1) The Assessment grossly overstates the number of businesses that will be covered by CCPA.
- 2) The evidence chosen to support conclusions about how many businesses will be covered is almost negligent in its scope: two, tiny, non-scientific surveys, the data from each of which has been manipulated to support a conclusion that could just as easily have supported a diametrically different result.
- 3) The Assessment relies on flawed reading of the actual underlying statute, SB 1121, and bases major conclusions on a fundamental misinterpretation of the text.
- 4) The Assessment lacks factual data, but nonetheless ascribes extraordinary costs to this law.
- 5) The regulatory impact statement is fatally flawed, and needs to start from scratch to more truly reflect actual details.

Please see attached for an in-depth analysis of the Impact Assessment Report.

All page references are to the original report (herein, the “Report”), which can be found at ([http://dof.ca.gov/Forecasting/Economics/Major\\_Regulations/Major\\_Regulations\\_Table/documents/CCPA\\_Regulations-SRIA-DOF.pdf](http://dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf)).



**A. Foundational incorrect assumption with respect to how many businesses would be covered by the law, resulting in incorrect assumption about costs.**

One of the three tests for which businesses are covered under CCPA reads: “[A business that] alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.”

- 1) The Report erroneously omits wording from the key definition of what constitutes a covered business by substituting “share” for “shares for commercial purposes”:
  - a. See page 7: “The CCPA applies to all businesses in California that meet one or more of the following three thresholds: (1) has annual gross revenues in excess of twenty-five million dollars (\$25,000,000). (2) buys, sells, or shares the personal information of 50,000 or more consumers, households, or devices. (3) derives 50% or more of its annual revenue from selling consumers’ PI.” [Emphasis added]
  - b. See page 20, section 2.1: “The law establishes three thresholds [for which businesses are required to comply with the CCPA], each of which would trigger compliance requirements if reached...2. A business buys, sells, or shares the personal information of more than 50,000 consumers, households, or devices per year” [Emphasis added]
  - c. See page 20: “A lack of data prevents us from estimating with precision the number of businesses that meet the other threshold requirements in the CCPA. However...any firm that collects personal information from more than 137 consumers or devices a day will meet the 50,000 threshold.” [Emphasis added]
  - d. As a result of the omission of “commercial purpose,” the Assessment fundamentally misreads the law, which applies to a business only if it is sharing information for a commercial purpose.
  - e. Thus, the proverbial blog that has 137 visitors a day is not covered by the law, unless the blog is collecting personal information and subsequently selling or sharing it for a commercial purpose.
    - i. Please note that an IP address alone does not qualify as PI, because an IP address **on its own** cannot identify a consumer.
    - ii. This means a blog could easily display contextual ads next to its subject matter (putting a garden shop ad next to a post about composting, for example) in such a way that no personal information is shared, meaning that it would not count toward the 137/day, 50,000/year threshold.
  - f. Also, note that even if one assumes a small business were making over 137 actual physical sales a day, which would thus meet the definition of ‘*sharing for a commercial purpose*,’ Section 1798.100(e) includes a **limitation** such that the right of access does not “*require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.*” In addition, Section 1789.110(d) reiterates that “*This section does not require a business to do the following: (1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained. (2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.*”

- i. This means that the entire Right to Know (right of access) is moot for businesses that are simply, for example, operating a store and making sales, unless the business is retaining the information in an effort to monetize it in the future by selling or disclosing it for a commercial purpose.
- ii. Especially with respect to the small online business, the reality is that if a business is simply showing an ad for a one-time transaction, and does not retain PI as part of that transaction, then there is no requirement for the business to keep that information with respect to that consumer, in order to be able to present it later in response to an access or opt-out or deletion request; and a one-time credit card transaction, if not maintained in a manner that would be considered personal information, is equally not covered by the law.
  1. Some have stated, incorrectly, that simply collecting an IP address as part of a visit to a website, constitutes collecting Personal Information under CCPA, but an IP address in and of itself is not PI because it alone cannot identify a consumer. So again, the notion that the small online business would be covered by CCPA even if it had as few as 137 visitors a day, is incorrect.
- iii. Yet, the vast bulk of the Report's costs are driven by the mistaken assumption that between 383,328 and 570,066 businesses will be covered because of this "sharing" test.

**B. Pure guess about how many businesses covered (p. 20): "We assume that either 50% or 75% of all California businesses that earn less than \$25 million in revenue will be covered under than CCPA."** The only backup the Report gives for this extraordinary claim is that "A survey completed by the International Association Privacy Professionals (sic) (IAPP) found that 8 out of 10 surveyed businesses believed that they would need to take compliance actions as a result of the CCPA."

- 1) There was no footnote to the report, but an IAPP/OneTrust survey "[Ready or not, here it comes: How prepared are organizations for the California Consumer Privacy Act?](#)" published in March 2019, surveyed 282 respondents, and has a chart titled "Nearly 8 in 10 respondents believe their employer must comply with the CCPA"; thus, we assume this is the IAPP report to which the authors refer.
- 2) Notably, **only 18% of the respondents in the IAPP survey were from companies with between 1 and 250 employees.**
  - a. Also notably, **21% of total respondents thought that CCPA did NOT apply to their businesses.**
  - b. There are no statistics in the IAPP survey that link these two answers, i.e., charting which respondents felt their businesses would have to comply with CCPA, against the size of the business the respondent represented.
  - c. Despite this lack of data, the Report authors somehow conclude from this IAPP study that at least 50%, and perhaps 75%, of all California businesses with less than \$25M in annual revenues, will have to comply with CCPA.
  - d. An equally plausible conclusion could have been that **no** businesses with under 250 employees felt they had to comply with CCPA—18% of the survey respondents were from companies with less than 250 employees, and 21% of respondents thought CCPA did not

apply to them. This is actually a more logical guess than the one the Report authors made (i.e., either 50% or 75% of all businesses would be covered by CCPA).

- i. To buttress this point, note that of those who thought CCPA did not apply to them, 89% thought that was either because their organization didn't collect/sell/disclose PI, or because it did not meet the definition of a business under CCPA.
  - ii. It is not clear what led the Report authors to conclude that the smaller businesses were *not* the ones who do not collect/sell/disclose PI, or meet the definition of a business under CCPA. There is literally no indication in the survey about this fact.
  - iii. **The entire conclusion of the Report depends on the authors' assessment of how many businesses are covered, and yet the statement that "the 50-75% upper-bound compliance range is reasonably supported by empirical evidence" is not supported by any empirical evidence—it is, in fact, simply a guess with no supporting evidence.**
- e. The result of this assumption, however, is that the Report concludes that somewhere between 383,328 and 570,066 California businesses will have to comply with CCPA (p. 23) at a cost of between \$11 billion and \$16.5 billion (page 29). This is a staggering extrapolation from what is essentially 'just one way to read a tiny, unscientific survey.'

**C. Absurdly high estimate of how many small California businesses covered (Line 761 of the SUSB): "[Number of Firms, Number of Establishments, Employment, and Annual Payroll by Enterprise Employment Size for States, NAICS Sectors: 2016](#)" report (choose "States, NAICS Sectors"), shows 745,791 California businesses with under 500 employees.**

- 1) Of that total, 465,078 have from 0-4 employees.
- 2) Thus, using the Report's 383,328 figure of how many firms will be covered by CCPA would mean that every single firm in California with over 5 employees, and 22% of the firms with between 1 and 4 employees, would be covered by CCPA.
- 3) Using the Report's 570,066 figure would mean that every single firm in California with over 5 employees, and 62% of the firms with between 1 and 4 employees, would be covered by CCPA.
- 4) Neither of these assumptions stand the test of common sense. There are 45,000 construction firms alone in California with between 0-4 employees, and 53,000 in health care and social assistance. Are the authors suggesting that tens of thousands of small contractors, or home health care firms, are businesses engaging in at least 137 transactions sharing personal information, every day, 365 days a year?
- 5) Small firms with under \$25M in revenue (which, using the Report's assumption of \$100,000 in revenue per employee, means firms with under 250 employees), **represent at least 97% of California firms**. The idea that some huge percentage of these firms are monetizing personal information by selling it, or sharing/disclosing it for a commercial purpose (excluding one-time transactions) defies belief. We may live in an information economy, but the vast majority of California firms with four or five employees are not data brokers mining consumer information and the vast majority of businesses are not making 50,000 sales a year—137 times a day, 7 days a week—day in and day out.
- 6) **In conclusion, we strongly disagree with the central thesis of the report that between 383,000 and 570,000 small businesses will be covered by CCPA. Indeed, the evidence presented to support this thesis is no better than a guess.**



- D. On page 11, there is another stunningly bold guess: “The total cost of initial compliance with the CCPA, which constitutes the vast majority of compliance efforts, is approximately \$55 billion. This is equivalent to approximately 1.8% of California Gross State Product in 2018.”
- No table is included in the report that totals to this \$55 billion figure.
  - It appears nowhere else, with no supporting backup as to how it was arrived at.
  - The paragraph outlining the \$55 billion figure, which is only mentioned once, begins with this statement: “we generate[d] a back of the envelope cost of CCPA compliance, including both the statute’s baseline costs and the incremental costs attributable to the regulations, using estimates from the TrustArc survey cited above.”
  - Reading the TrustArc survey the Report relies on, and upon which this entire conclusion was based, it turns out that TrustArc surveyed NO companies with under 500 employees, and only 68 companies with between 500 and 1,000 employees. 68 companies, nationally.***
  - Let us reiterate: The Report had NO DATA on 99.8% of California businesses, the ones with under 500 employees—and yet it ascribes tens of billions of dollars in costs to these businesses.*** [Note: [California EDD data](#) (choose ‘Number of Businesses, Number of Employees, and Payroll by Size of Business (Table 1)’ and [US Census](#) data diverge here, but the point is there are a tiny number of very large firms, and a huge number of small ones.)]
  - The Report does say in a footnote to this section that “The TrustArc survey only sampled privacy professionals from firms with at least 500 employees. **Therefore, it is very possible that we are overestimating the compliance costs for smaller firms.**”
  - That a formal economic report, ascribing billions of dollars in costs, would not have any data on 99.8% of California businesses, is astounding.
- E. **Errors:** On page 23, the Report incorrectly states that the total number of firms with over 500 employees in California, is 9,858. It also incorrectly identifies the Survey of US Businesses data from which this total is drawn, as the 2017 Survey of US Businesses (SUSB). In fact, it is the [2016 data, released on 12/18/2018](#). Please go to the “States, NAICS Sectors” spreadsheet for the underlying data.
- The correct total for California businesses with more than 500 employees is found on line 762 of the “Number of Firms, Number of Establishments, Employment, and Annual Payroll by Enterprise Employment Size for States, NAICS Sectors: 2016” sheet. **This number is 6,191, whereas the Report uses a figure 60% higher (9,858).**
  - Every state’s total for numbers of businesses with over 500 employees on that spreadsheet, is higher than the individual totals by NAICS Code totals, by a substantial amount, and while the employment totals tally, the actual number of businesses do not, presumably because of multi-sectorial businesses.
  - This change has a consequence of overstating the costs in the report ascribed to large businesses, by 60%.
  - The [EDD figures](#) are even starker, and the number of California businesses with over 500 employees is only 2,687.
  - However, the conclusion is clear: there are nowhere near 9,000+ businesses in California with over 500 employees.

**In sum, we offer the following conclusions:**

- 1) There is no backup for the \$55B figure on page 11, i.e. the ‘total cost of initial compliance with the CCPA;’ especially in light of the IAPP survey that the authors rely on, which states that as of early 2019, 65% of surveyed firms self-rated as being either medium-prepared, or highly-prepared, for CCPA compliance. If the firms are representative of the firms in California—which the authors imply by using other parts of the survey to determine how many businesses in California will be covered—then it appears that 2/3 of the respondents were already halfway prepared to comply with CCPA. So how does the \$55B figure fit into this narrative? Are the authors suggesting this will be an *additional* \$55B?
- 2) The IAPP survey shows 39% of firms at medium preparedness, and 26% at high preparedness.
  - a. If we assume that medium = 50% prepared; and ‘highly’ = 80% prepared, then mathematically this works out to businesses having done about 40% of the total workload (the IAPP chart is titled “Organizations are about halfway to CCPA compliance”).
  - b. This would then imply that roughly \$22B in compliance costs have already been spent in California complying with CCPA, and yet the Report makes no mention of evidence supporting this thesis—and a reasonable reader might be surprised to have seen no stories about \$22B in compliance costs incurred *in the last 14 months* since CCPA passed into law.
  - c. The Report does say that “standards and compliance for the GDPR have already imposed costs on many firms that operate in California. This reduces their expected cost of CCPA compliance...” but it does not attempt to quantify this reduction, nor to explain if that has reduced or will reduce the \$55B cost figure.

We request that you withdraw the Report, or at least correct its most blatant errors:

- Misused definition of Section 1798.140(c)(1)(B), i.e. substituting ‘share’ for ‘shares for commercial purposes,’ and the incorrect assumption that merely collecting an IP address from 137 visitors a day would qualify a business to become a covered entity. This is incorrect per the black letter definitions in the law, and as a result, the number of covered businesses is vastly overstated.
- Correcting the ‘guess’ that between 383,000 and 570,000 small businesses will need to pay significant compliance costs as a result of this law, justified simply because of a survey of 282 US respondents in which 20% of the respondents represented small businesses, and 20% thought CCPA would not apply to their businesses. Relying on a tiny sample size to arrive at an outcome suggesting hundreds of thousands of firms could be covered, which could equally have been vastly smaller, is simply guessing without any reasonable basis. One responsible course of action here could have been to provide a range of outcomes, from no covered firms, to all businesses in California covered by the law, and then to state that there is not enough data to know what the cost would be.
- Correcting the errors with respect to the NAICS data, which overstates how many large businesses will be covered by as much as a third (especially if cross-referenced with the EDD data, which would see the Report overstate the number of large businesses by almost 3X).
- Removing the \$55B figure to comply with CCPA, or providing backup; and explaining why, if the same survey the authors used to arrive at the number of covered businesses, states that 40% of the compliance work has already been done, the authors make no mention of that cost reduction.

Attorney General Becerra  
November 19, 2019  
Page 7

In conclusion, we were disappointed with the quality of work in the Report, which takes an authoritative tone in attempting to pass off guesswork as detailed fact-based research.

Yours sincerely,

/s/ Alastair Mactaggart, Chair

Californians for Consumer Privacy