CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

TIM DAY
SENIOR VICE PRESIDENT
CHAMBER TECHNOLOGY
ENGAGEMENT CENTER (C_TEC)

HAROLD KIM
CHIEF OPERATING OFFICER
U.S. CHAMBER INSTITUTE
FOR LEGAL REFORM

March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA90013

Re: California Consumer Privacy Act Rulemaking

Dear Attorney General Xavier Becerra:

The U.S. Chamber of Commerce ("Chamber") and the U.S. Chamber Institute for Legal Reform ("ILR") respectfully submit these comments in response to the public forums hosted by the Attorney General. The Chamber recognizes the importance of consumer privacy, and for this reason, it recently released model privacy legislation[1] which includes a nationwide privacy framework that protects privacy based upon risk to consumers, encourages transparency, and promotes innovation through collaboration between government and private stakeholders. As you continue to adopt regulations and the Legislature pursues further action in response to the California Consumer Privacy Act ("CCPA" or "Act"), the Chamber urges you to consider the principles espoused by the model legislation in order to develop greater certainty for both consumers and business.

I. CONSUMERS BENEFIT FROM THE DATA-DRIVEN ECONOMY

The data-driven economy continues to have a tremendously positive impact for consumers and the national economy, and in particular for California. The information sector contributed over $271 million in 2017 to California's GDP[2] and accounted for nearly 543,000 jobs[3] in the state in 2018. While the industry sector numbers alone are impressive, the Chamber recognizes the fact that

---

[1] *See* U.S. Chamber of Commerce Model Privacy Bill (February 13, 2019) *available at* https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf. (*hereinafter* "Model Bill").
[2] *See* "GDP and Personal Income," U.S. DEPARTMENT OF COMMERCE, BUREAU OF ECONOMIC ANALYSIS (2017) *available at* https://apps.bea.gov/iTable/iTable.cfm?reqid=70&step=30&isuri=1&major_area=0&area=06000&year=2017&tableid=505&category=1505&area_type=0&year_end=-1&classification=naics&state=0&statistic=-1&yearbegin=-1&unit_of_measure=levels.
[3] *See* "Economy at a Glance—California," U.S. DEPARTMENT OF LABOR, BUREAU OF LABOR STATISTICS (Dec. 2018) *available at* https://www.bls.gov/eag/eag.ca.htm#eag_ca.f.4.

data-driven innovation is changing and benefiting consumers that receive products and services from every sector.

The value of the digital economy has a significant effect on the national economy and the welfare of individual Americans. For example, according to one study, digital advertising was projected to overtake other forms of ads this year, topping over $100 billion in value.[4] Data-driven services are beneficial to consumers. For example, the vast majority of Americans prefer targeted advertising.[5] Revenues obtained by providers from advertisers help reduce prices consumers must pay for products and services.[6]

In addition to direct commercial benefits for consumers, the private sector's use of data is improving society. California localities are partnering with private companies to install gunshot detection technology in order to save lives and enhance public safety.[7] Data obtained through social media can also be used to prevent and contain disease outbreaks.[8]

The Federal Trade Commission, across administrations, has explained that the appropriate use of consumer data not only results in more efficient markets, it has the potential to "create opportunities for low-income and underserved communities."[9] Financial services companies are now using data to widen the pool of applicants that have access to credit.[10]

Data is changing mobility as well. In the future, autonomous vehicles, which have the potential to reduce the 40,000 road fatalities each year (of which 94 percent are caused by human error),[11] will potentially use and transmit up to 4 terabytes of data per day.[12] This technology will be of particular benefit to the elderly, the blind, and the economically disadvantaged as it will increase their mobility whether for purposes of gaining employment or visiting loved ones.

---

[4] Sean Fleming, "Digital now accounts for half of all US advertising," World Economic Forum (Oct. 18, 2018) *available at* https://www.weforum.org/agenda/2018/10/digital-now-accounts-for-half-of-all-us-advertising/.

[5] *See* IAB, "The Value of Targeted Advertising to Consumers," (citing 2016 survey stating 71 percent of consumers prefer targeted advertising) *available at* https://www.iab.com/wp-content/uploads/2016/05/Value-of-Targeted-Ads-to-Consumers2.pdf.

[6] Laurence Green, "Does advertising increase consumer prices?" Advertising Association, *available at* https://www.adassoc.org.uk/advertisings-big-questions/does-advertising-increase-consumer-prices/.

[7] Ryan Johnston, "Gunshot detection expands reach in California city to cover campuses," *State Scoop* (Feb. 23, 2018) *available at* https://statescoop.com/fresno-police-department-extend-contract-with-gunshot-detection-system-company/).

[8] Dr. Utz Lederbogen, "Predicting flu epidemics with Twitter data-Cooperation between Onsabruick University and IBM," Informationsdienst Wissenshaft (Mar. 8, 2019) *available at* https://idw-online.de/de/news657258.

[9] Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion?* 5-6 (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[10] Ann Carnns, "New type of credit score aims to widen pool of borrowers," *The Seattle Times* (Nov. 3, 2018) *available at* https://www.seattletimes.com/business/new-type-of-credit-score-aims-to-widen-pool-of-borrowers/.

[11] *See* Chamber Technology Engagement Center Comments to Department to Transportation at 1-2, *In the Matter of Automated Vehicle Policy Summit* (Mar. 9, 2018) *available at* https://www.uschamber.com/sites/default/files/c_tec_av_3.0_comments_1.pdf.

[12] Kathy Winter, "Meaning Behind One Big Number: 4 Terabytes," Intel Newsroom (Apr. 14, 2017) *available at* https://newsroom.intel.com/editorials/self-driving-cars-big-meaning-behind-one-number-4-terabytes/.

The information-driven economy will also require massive investment in communications infrastructure. The 5G networks that will transfer the mass amounts of data necessary to power smart cities and the Internet of Things could produce over 3 million new jobs and $500 billion in increased GDP over the next decade.[13]

Data and laws regulating privacy affect *every* industry and it is important that policymakers recognize regulations should be flexible to address this reality. The retail, financial services, insurance, transportation, communications, entertainment, health, energy, and manufacturing sectors all rely on data and are impacted by its regulation. California is home to nearly one tenth of the nation's *Fortune 500* companies[14], representing a wide variety of industries, which all use data in order to improve the products and services they offer to their customers. Any regulation imposed upon data collected, used, or shared by California businesses or about California residents has far-reaching national implications, and it is for this reason that the U.S. Chamber of Commerce offers its comments to improve how the CCPA operates.

II. THE ATTORNEY GENERAL'S RULEMAKING SHOULD DRAW UPON THE CHAMBER'S CONSENSUS PRINCIPLES.

a. The Chamber's Proposal

The U.S. Chamber of Commerce convened over 200 member companies and trade associations to release model privacy legislation based upon its privacy principles[15] and elements of CCPA. Although the Chamber supports a federal privacy law, the business community believes that its privacy principles should be instructive to the current rulemaking.

Given the effect of data on interstate commerce and US economic prosperity, today's current technological and state regulatory environment necessitates a federal privacy law that preempts state and local privacy laws. A national privacy framework also will bolster continued U.S. leadership in trade internationally and facilitate interoperable cross-border data transfer frameworks. Policies that promote the free flow of data across state and national borders will facilitate numerous consumer benefits, economic growth, and trade.

While the best approach is one national privacy framework, the Chamber offers its suggestions for ways to improve and enhance California's already-enacted privacy law. The Chamber believes that privacy protections should be risk-focused. Privacy protections should be considered in light of the benefits provided to consumers and the economy and the privacy risks presented by the data being used, and the way a business uses it. Enforcement should focus on cases in which consumers suffer actual harm, as opposed to mere speculative injuries or technical

---

[13] *See* Accenture Strategies, "Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities," at 1 (2017) *available at* https://www.accenture.com/t20170222T202102__w__/us-en/_acnmedia/PDF-43/Accenture-5G-Municipalities-Become-Smart-Cities.pdf.

[14] "Number of U.S. companies listed in the Fortune 500 in 2018," Statista (2019) *available at* https://www.statista.com/statistics/303696/us-fortune-500-companies-by-state/.

[15] U.S. Chamber of Commerce Privacy Principles (Sept. 6, 2018) *available at* https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf.

violations of the law. The Chamber's privacy legislation discussion draft draws upon these principles.

At the same time, the Chamber agrees with the fundamental privacy protections offered by CCPA and believes that consumers should have a say as to how personally identifiable information about them is shared. That is why the Chamber's model legislation offers consumers the ability to opt out of data sharing with third parties. At the same time, companies using and sharing consumer data should be able to continue innovating and not be hindered by consumer consent outcomes and regulations that do not take into consideration the risks and benefits of data.

Consumers, upon verified request, should be given the qualified ability to request that information about them be deleted. Any proposed right of deletion, like the CCPA, must allow for reasonable exceptions to such requests. Data deletion rights though should not impede a company's ability to, among other things, provide the goods or services for which a consumer and business contract, maintain good data hygiene, conduct security-protected research, combat fraud and security threats, and comply with legal obligations.

b. The Definition of "Personal Information"

The definition of "personal information" is the capstone of any privacy framework. The Chamber urges the Attorney General to take great care in interpreting this important definition. The Act generally defines "personal information" as:[16]

> [I]nformation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked directly or indirectly, with a particular consumer or household…

Specifically, the Chamber supports a definition of "personal information" that is not overly expansive and could capture data that is not truly personal. The Chamber recommends that personal information should be defined as "information that identifies a consumer."[17] Privacy regulators should avoid overly-expansive definitions of "personal information" and not focus on data that could hypothetically be connected to an individual. Similarly, the Chamber cautions against an expansive view of the definition of "household" which could create confusion for both consumers and businesses.

The Chamber also recognizes that certain practices that work to eliminate connecting data to and preventing harm to individuals should not be considered "personal information." For example, the Chamber generally suggests that aggregated, de-identified and pseudonymous data should not

[16] SB 1121 § 9(o)(1) (2018).
[17] *See* Model Bill at § 1(7).

be considered "personal information." The CCPA and the Chamber both support similar definions of "pseudonymizaiton":[18]

> [I]nformation process in such a manner that it can no longer be attributed to a specific consumer without the use of additional information, provided that such additional information is kept separately and is subject to technical and organization measures to ensure that the personal information do not identify, or cannot reasonably identify, a natural person.

California should interpret "personal information" to exclude pseudonymized information. As a matter of public policy, the Attorney General should encourage companies to protect information through innovative means. In fact, the General Data Protection Regulation in Europe promotes the use of pseudonymization as means to protect individual privacy.[19]

The CCPA also carves out "publicly available information" from the definition of "personal information."[20] The Chamber urges the Attorney General to interpret the term "publicly available information" in a manner that protects the First Amendment rights of those who process and share personal information.

c. Definition of Consumer

Finally, the Chamber advocates for exempting information pertaining to employees from obligations under the CCPA. Specifically, business records about an employee's job duties cannot be subject to regulations that allow an individual to request to review or delete identifying data about them. Interpretation of the Act should not include obligations for employees or contractors of a business acting in their role as employee or contractor.

d. Protection of Loyalty Programs

The Chamber requests that the Attorney General also consider the impact that CCPA will have on consumer loyalty programs. These loyalty programs offered by retailers, banks, airlines, restaurants, and entertainment companies greatly benefit consumers. According to one study, the overwhelming majority of consumers agree that loyalty programs save them money.[21]

California's Act has fomented uncertainty in the business community about its impact on loyalty programs. Section 6 of the CCPA amends California law to prohibit businesses from discriminating against a consumer because a consumer exercised any of the consumer's privacy

---

[18] *See* Model Bill § 1(8); *See also* SB 1121 § 9(r).

[19] *See* Recital 28 General Data Protection Regulation ("The application of pseudonymization to personal data can reduce the risks to data subjects concerned and help controllers and processors to meet their data-protection regulations.").

[20] *See* SB 1121 at § 9(0)(2).

[21] Emily Collins, "How Consumers Really Feel About Loyalty Programs," FORRESTER (May 8, 2017) *available at* http://www.oracle.com/us/solutions/consumers-loyalty-programs-3738548.pdf.

rights under the Act[22] According to the Act, discrimination could be done in the form of denying goods or services, "charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposes penalties," or differing levels of quality.[23] The Chamber strongly urges the Attorney General to interpret that the loyalty programs that consumers overwhelmingly enjoy and benefit from are not negatively impacted by Section 6 of the CCPA and are not considered to discriminate against a consumer for exercising privacy rights. We urge the Attorney General and the Legislature to protect these consumer-friendly programs.

III. DATE OF ENFORCEMENT

Currently, the CCPA states that "the Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner."[24] The Chamber additionally requests that the Attorney General clarify that, when enforcement starts, any enforcement that occurs will only be based on business conduct or alleged business non-compliance that takes place on or after the enforcement date. Enforcement should not be based on conduct that occurs between the effective date—January 1, 2020—and the enforcement date of the Act.

IV. CALIFORNIA'S APPROACH TO ENFORCEMENT MAY BE INCONSISTENT WITH BEST PRACTICES AND IS UNLIKELY TO IMPROVE DATA PRIVACY.

There are laudable parts of the CCPA and California is influencing national discussions about privacy. But there are some areas of significant concern, especially from an enforcement perspective. Enforcement mechanisms are a key component of any legal regime. The CCPA contemplates enforcement by the Attorney General. It also contemplates enforcement through a private right of action for the "unauthorized access and exfiltration, theft, or disclosure" of "nonencrypted or unredacted personal information" "as a result of [a] business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[25] The private right of action authorizes uncapped statutory damages "in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater."[26]

There are well-documented problems with this sort of approach. *First*, enforcement provisions of data privacy laws should only apply where there is demonstrable, concrete harm to individuals proximately caused by a violation of the statute.[27] When it enacted the CCPA, the Legislature expressed its intent to prevent "devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm" that

[22] *See* SB 1121 at § 6.
[23] *Id.*
[24] *See* § 1798.185(c).
[25] § 1798.150(a)(1).
[26] § 1798.150(a)(1)(A).
[27] *See Privacy Principles*, at 2; *cf. Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1550 (2016) (dismissing suit for lack of standing where plaintiff alleged a "procedural violation" of the Fair Credit Reporting Act but no "concrete harm").

might result from a data breach.[28] These are worthy goals, but the text of CCPA's private right of action does not clearly require a showing of harm, setting the stage for the type of enforcement drift and litigation abuse we have seen under certain federal statutes.[29]

Second, experience shows that private rights of action coupled with uncapped statutory damages invite abusive litigation seeking jackpot paydays for plaintiffs' attorneys rather than improved outcomes for consumers. That problem is magnified where, as here, there is no clear statutory requirement for a potential plaintiff to show concrete harm, and lawyers are incentivized by statutory damages to cobble together class actions seeking enormous payouts for *de minimus* procedural or technical violations of the statute.

The federal Telephone Consumer Protection Act ("TCPA") provides a cautionary example. Although that statute was designed to target unscrupulous scam telemarketers, trial lawyers often uses it to bring cases against legitimate American businesses, big and small, that are often simply attempting to reach out to their own customers using numbers provided by those customers.[30] For example, in a recent case examining a rule promulgated under the TCPA, the D.C. Circuit expressed shock that a pharmaceutical company might be held liable in state court for $150 million in damages for a seemingly benign error like "failing to include opt-out notices on faxes that the recipients had given [the company] permission to send."[31] Unfortunately, such astronomical figures are common in the TCPA context and the plaintiffs' bar frequently assembles classes based on similarly innocent mistakes. Some have even built a cottage industry of victims that let calls—and damages accrue—to secure larger payouts. ILR believes companies should be held responsible when negligent mistakes result in harm. But permitting suits for uncapped statutory damages where there is no showing of harm is a recipe for abusive litigation that stifles economic growth and innovation.

Because the Legislature is considering amendments to the CCPA, California has an opportunity to correct problems with the CCPA before the law goes into effect. Unfortunately, press reports indicate that that you are seeking legislative amendments that would make the statute *worse*, not better, by deleting a provision which gives companies an opportunity to cure data breaches within 30 days, and by creating new liability for violations that are unrelated to the disclosure of personal information.[32] Your proposal reportedly also would eliminate the ability of companies to seek guidance from the Attorney General on how to comply with certain vague

---

[28] AB 375 § 2 (2018).

[29] *See, e.g.*, ILR, *The Juggernaut of TCPA Litigation: The Problems with Uncapped Statutory Damages* 1 (2013) ("*Juggernaut*") ("It is rare these days to see TCPA litigation brought against its original intended target—abusive telemarketers."), *available at* https://www.instituteforlegalreform.com/uploads/sites/1/TheJuggernautofTCPALit_WEB.PDF.

[30] *See* ILR, *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits* 2 (2017), *available at* https://www.instituteforlegalreform.com/uploads/sites/1/TCPA_Paper_Final.pdf.

[31] *See Bais Yaakov of Spring Valley v. FCC*, 852 F.3d 1078, 1081 (D.C. Cir. 2017) ("Let that soak in for a minute: Anda was potentially on the hook for $150 million for failing to include opt-out notices on faxes that the recipients had given Anda permission to send."), *cert. denied*, 138 S. Ct. 1043 (2018).

[32] *See, e.g.*, Alexei Koseff, *California attorney general looks to expand new data privacy law*, San Francisco Chronicle (Feb. 25, 2019), https://www.sfchronicle.com/politics/article/California-attorney-general-looks-to-expand-new-13644242.php.

provisions in the CCPA, raising significant due process concerns.[33] Such moves would reduce incentives to engage in reasonable privacy risk management, which is a key part of standards like those promulgated by the National Institute of Standards and Technology (NIST) in the United States Department of Commerce.[34]

ILR has also seen mention of proposals to authorize localities to bring lawsuits under the CCPA. Authorizing municipal lawsuits would be a mistake. It would threaten the administration of justice by diverting awards away from consumers and into municipal coffers. Worse, by incentivizing localities to bring speculative claims in the hope of large payouts, it would dilute the judicial resources allocated to potentially meritorious claims. Fundamentally, authorizing municipalities to bring lawsuits to enforce state law upsets the traditional balance of power between local and state government and threatens California's role in setting state policy.[35]

Attorneys are already gearing up to bring a wave of injury-free lawsuits over privacy and technology issues.[36] The *in terrorem* effect of vague obligations and multimillion-dollar judgments will not improve consumer welfare. Such proposals will undermine a successful data privacy policy and divert resources from risk-based compliance efforts into litigation that enriches lawyers but does not protect consumers.

Our shared goal should be, as the Chamber and ILR have explained, a regulatory regime that facilitates transparency and predictability for consumers and encourages collaboration and constant improvement.[37] Thus, enforcement should be focused on harm to consumers, with discretion vested in the government, not private actors or local governments. It should be predictable and reward prudent risk management. And, it should ensure that damages are commensurate with harm.[38] Additionally, the Attorney General should remain available as a resource to private organizations that want guidance. California should revise the CCPA to reflect these principles.

---

[33] *See id.*; *cf. Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 158–59 (2012) ("It is one thing to expect regulated parties to conform their conduct to an agency's interpretations once the agency announces them; it is quite another to require regulated parties to divine the agency's interpretations in advance or else be held liable when the agency announces its interpretations for the first time in an enforcement proceeding[.]").

[34] In its recent revision to Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, at 8, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf NIST observed that "[w]ithout adequate risk management preparation at the organizational level, security and privacy activities can become too costly, demand too many skilled security and privacy professionals, and produce ineffective solutions." Efforts across government support privacy risk management, such as the Privacy Framework that NIST intends to be a tool for use across the economy. *See, e.g.*, *Live Webinar: Outlining the NIST Privacy Framework*, https://www.nist.gov/news-events/events/2019/03/live-webinar-outlining-nist-privacy-framework

[35] *Cf. California Redevelopment Assn. v. Matosantos*, 267 P.3d 580, 597 (Cal. 2011) ("In our federal system the states are sovereign but cities and counties are not; in California as elsewhere they are mere creatures of the state and exist only at the state's sufferance." (citation omitted)).

[36] *See* Brief of Amici CTIA–The Wireless Association® et al. at 11, *FCA US LLC v. Flynn*, No. 18-8010 (U.S.), *available at* https://www.wileyrein.com/assets/htmldocuments/SCOTUS%20Motion%20and%20Amicus%20Brief%20-%20Hacking%20Suit%2010.30.2018%20003.pdf (describing reports of plaintiffs firms "salivating" over the prospect of privacy and security litigation)

[37] *See Privacy Principles*, at 2.

[38] *See id.*; *see also Juggernaut*, at 12 (explaining the success of regimes with reasonable damages caps).

V. THE RULEMAKING SHOULD PROVIDE REGULATORY SAFE HARBORS THAT OFFER PREDICTABILITY, ENCOURAGE BEST PRACTICES, AND LIMIT LIABILITY UNDER ANY PRIVATE RIGHT OF ACTION.

The CCPA's private right of action creates potential liability for a business's "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information" where that violation results in the disclosure of "nonencrypted or nonredacted personal information."[39] To secure passage of the CCPA, privacy advocates assured lawmakers that this language was designed to create statutory "safe harbors" that would protect businesses operating in good faith and taking reasonable precautions to protect their customers' data from disclosure.[40]

Safe harbors are routine in California and elsewhere to encourage good behavior and provide predictability. Examples abound.[41] Safe harbors will be particularly useful in addressing privacy and data security practices, which often are built into product and service offerings with longer lifecycles, and also may need to evolve over time to meet shifting threats and challenges. Safe harbors have been effectively used in the context of global data transfers,[42] Internet platform operations,[43] the regulation of marketing to children,[44] compliance with anti-kickback laws,[45] and numerous other settings. Safe harbors can take the form of immunities from suit, or they can be affirmative defenses, as in the case of Ohio's new cybersecurity regime, which protects organizations from liability if they have taken certain actions.[46]

---

[39] § 1798.150(a)(1).

[40] *See Understanding the Rights, Protections, and Obligations Established by the California Consumer Privacy Act of 2018: Where should California go from here?: Informational Hearing Before the Comm. On Privacy and Consumer Protection*, 2019 Leg. Sess. (Cal. 2019) (statement of Alastair Mactaggart, Chairman, Californians for Consumer Privacy, explaining purpose of safe harbor provisions), *available at* https://www.assembly.ca.gov/media/assembly-committee-privacy-consumer-protection-20190220/video.

[41] *See Lopez v. Nissan N. Am., Inc.*, 201 Cal. App. 4th 572, 592 (2011) (recognizing that state law in "provides a safe harbor against UCL claims complaining about the accuracy of odometers"); *Bourgi v. W. Covina Motors, Inc.*, 166 Cal. App. 4th 1649, 1661 (2008) (noting that "[t]he California Legislature has provided as a matter of policy that new vehicle dealers are afforded a safe harbor by complying with the damage disclosure law"). Likewise, Proposition 65 has safe harbors, *see, e.g.*, *Envtl. Law Found. v. Wykle Research, Inc.*, 134 Cal. App. 4th 60, 66, (2005). "When specific legislation provides a 'safe harbor,' plaintiffs may not use the general unfair competition law to assault that harbor." *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 182 (1999).

[42] *See, e.g.*, Federal Trade Commission, *U.S.-EU Safe Harbor Framework* (Sept. 4, 2015), https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

[43] *See, e.g., UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1036 (9th Cir. 2013) (applying "safe harbor" protection under the Digital Millennium Copyright Act)

[44] *See* Federal Trade Commission, *Children's Online Privacy Protection Act Safe Harbor Program* (last visited Mar. 8, 2019), https://www.ftc.gov/safe-harbor-program.

[45] Federal "'safe harbor' regulations describe various payment and business practices that, although they potentially implicate the Federal anti-kickback statute, are not treated as offenses under the statute." https://oig.hhs.gov/compliance/safe-harbor-regulations/index.asp

[46] Ohio S.B. 220, Data Protection Act, providing a "safe harbor" for companies that implement a program that complies with the Framework for Improving Critical Infrastructure Cybersecurity developed by NIST. Business can choose from frameworks, including NIST SP 800-171, NIST SP 800-53 and 800-53(a), the Federal Risk and Authorization Management Program (FedRAMP), Center for Internet Security (CIS) Critical Security Controls, the ISO 27000 Family, the HIPAA Security Rule, Graham-Leach-Bliley Act, or the Federal Information Security Modernization Act (FISMA).

The Attorney General should make good on the Legislature's intent by seeking comment on the scope of the CCPA's safe harbors and clarifying that they are intended to protect businesses.[47] *First*, the rules promulgated by the Attorney General should address the promised safe harbor for businesses that "implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[48] The rules should clarify that this standard is met when a business adopts information or data security practices that are recommended by an appropriate body such as an industry specific regulator or trade association,[49] or when businesses can otherwise show that they have made good faith efforts to adopt compliance programs appropriate for the risks associate with the data they maintain.[50]

Second, the rules promulgated by the Attorney General should address the statutory safe harbors for "[e]ncrypted" or "[r]edacted" "personal information."[51] In addition, because the CCPA incorporates an existing statutory definition of "personal information" as (1) an "individual's first name or first initial and his or her last name in combination with" any one of several statutorily identified data elements "when either the name or the data elements are not encrypted or redacted" or (2) a "username or email address in combination with a password or security question and answer that would permit access to an online account,"[52] the rules should clarify that the safe harbors cover partially encrypted or redacted information where at least one element is redacted or encrypted and the unencrypted or unredacted data is either publicly available or cannot be linked with any specific individual.

Third, the rules promulgated by the Attorney General should clarify that a business that implements "reasonable security procedures and practices" following a data breach will be found to have "cured" the breach within the meaning of the CCPA.[53] As currently enacted, the CCPA is designed to afford businesses 30 days to cure a data breach and thereby to avoid "individual statutory damages or class-wide statutory damages"[54] Affording businesses this reasonable

---

[47] *See* §§ 1798.155(a) ("Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title"), 1798.185(c) ("The Attorney General may adopt additional regulations as necessary to further the purposes of this title.").

[48] § 1798.150(a)(1).

[49] For example, the U.S. Department of Health and Human Services has issued voluntary cybersecurity guidelines to reduce cybersecurity and data breach risks for health care organizations of varying sizes. *See* HHS, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (2019), *available at* https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf. Similarly, the Communications Security, Reliability and Interoperability Council, a federal advisory committee operating under the auspices of the Federal Communications Commission, regularly develops security recommendations for entities in the telecommunications industry. *See, e.g.*, FCC, *Communications Security, Reliability and Interoperability Council VI* (Jan. 3, 2019), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-0. Businesses that demonstrate compliance with such standards are engaging in reasonable security procedures and practices, and the Attorney General's interpretation of the CCPA should reflect that reality.

[50] *See Privacy Principles*, at 1 (explaining that "data controls should match the risk associated with the data and be appropriate for the business environment in which it is used.").

[51] § 1798.150(a)(1).

[52] *See* Cal. Civ. Code § 1798.81.5(d)(1)(A).

[53] § 1798.150(a), (b).

[54] § 1798.150(b).

opportunity to cure deficiencies before private action is initiated will encourage greater transparency and cooperation between businesses, regulators, and consumers.[55] The rulemaking should therefore strengthen this commonsense cure provision by clarifying the Attorney General's interpretation that adoption of an appropriate security program is sufficient to cure an actionable disclosure. Even with such a clarification, businesses will remain eager to adopt appropriate security programs ex ante; in addition to the negative publicity that often accompanies a data breach, the CCPA makes clear that a plaintiff may still recover "actual damages" independent of any cure.[56]

VI. CONCLUSION

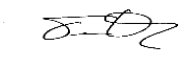
Data is important to every business in the United States whether it be credit reporting companies enabling consumers to be able to access credit in a matter of minutes as opposed to days, marketers presenting tailored products and services to consumers, or automakers and technology firms contributing to the reduction of traffic deaths. Effective, innovative, and responsible use of data is improving the lives of Americans in significant ways. Large amounts of data are being used, analyzed, and shared to bring about these positive societal and economic changes, and companies must respect the privacy of individuals.

While a national privacy standard is preferable, the Chamber recognizes the important work being done in California to protect consumer privacy and asks that the Attorney General interpret CCPA from a risk-based perspective that protects consumers while promoting innovation. California should seek to avoid overly expansive definitions of personal information and protect popular consumer loyalty programs.

The U.S. Chamber Institute for Legal Reform urges California to amend the CCPA to ensure that its enforcement regime is focused on actual harm to consumers and not on incentivizing potentially destructive litigation that does little to help consumers. Consistent with that goal, ILR urges the Attorney General to consider in the current rulemaking the means outlined above for strengthening the statutory safe harbors enacted by the Legislature.

The Chamber and ILR stand ready to work with the Attorney General to protect consumer privacy and innovation.

Respectfully Submitted,



Tim Day
Senior Vice President
Chamber Technology Engagement Center

Harold Kim
Chief Operating Officer
U.S. Chamber Institute for Legal Reform

[55] *See Privacy Principles*, at 2.
[56] § 1798.150(b).