

Message

From: Amy Zajac-Hamerton [REDACTED]
Sent: 3/8/2019 3:55:42 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Comments on CCPA From Genentech, Inc
Attachments: Genentech_Comment_Letter_March_8_2019.pdf

To Whom it May Concern:

Genentech is submitting the attached comments in regards to the California Consumer Privacy Act (CCPA) of 2018. Should you have any questions or need additional information from Genentech, my contact information is below.

May I please request confirmation of this email. Thank You.

Amy Zajac
State Government Affairs
[REDACTED]

Genentech
A Member of the Roche Group

March 8, 2019

LEGAL DEPARTMENT

By Email to: PrivacyRegulations@doj.ca.gov

The Honorable Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Re: Genentech CCPA Implementation Proposals

Dear Attorney General Becerra:

Genentech, Inc. (“Genentech”)¹ submits these comments in furtherance of your office’s broad rulemaking authority under the California Consumer Privacy Act (“CCPA”).² This letter identifies Genentech’s priority concerns with certain ambiguous, unclear, incomplete, or overbroad language found in the CCPA and presents preliminary rulemaking recommendations to address those concerns.

Genentech and similarly situated life science companies play a critical role in advancing healthcare in California and throughout the world.³ Collectively, Genentech and other Roche group companies employ over 13,000 Californians in 10 facilities throughout the state.⁴ We strive to enhance personalized patient care and access to innovative medicines through our work, and have a strong commitment to advancing science and improving public health globally. The work of our scientists, clinicians, and other employees encompasses innovative basic and clinical research, biopharmaceutical medicine development and manufacturing, and programs to increase patient access to appropriate medicines and services.

Our primary concerns with the CCPA have to do with its general applicability to biotechnology and life science companies, like Genentech, which currently follow many rigorous privacy laws⁵ that do not impact businesses in other industries. Genentech and other biotechnology companies already must commit significant resources, including the implementation of systems, policies and safeguards to ensure that personal data is responsibly protected, and in a compliant manner. In other words, biotechnology companies *already* engage in advanced data protection practices.

¹ All references to “Genentech” in this letter refer to Genentech, Inc., with headquarters in South San Francisco, a member of the Roche group of companies, and the California based, United States affiliate of F. Hoffman-La Roche, Ltd.

² California Civil Code §§ 1798.185(a) and (b).

³ The Roche group of companies is active in over 100 countries worldwide.

⁴ Figures reported as of February 21, 2019, and reflect Roche group numbers for California.

⁵ Existing privacy laws include HIPAA (Health Insurance Portability and Accountability Act of 1996), the CMIA (California’s Confidentiality of Medical Information Act), and similar international privacy requirements, including the GDPR (General Data Protection Regulation) in Europe.

Although Genentech understands the importance of privacy guidance for business use of personal data, it will be extremely challenging, absent clarifying regulations, to harmonize the CCPA requirements with other privacy law requirements. Further, as applied to Genentech and similar companies, we believe the CCPA will provide only marginal additional privacy benefit to individuals, and at the expense of unduly burdening companies engaged in critical healthcare related efforts on which Californians and people around the world depend. Consequently, as an overarching principle, we respectfully propose that wherever possible, the Attorney General seek to harmonize CCPA implementation with existing laws, including HIPAA and the GDPR.

We recognize that the CCPA, as amended, includes certain exemptions for data with a nexus to healthcare. Such carve-outs include an exemption for information that is already regulated by HIPAA or the CMIA, as well as information collected as part of a clinical trial. We believe these exemptions reflect two general principles. First, the California legislature recognizes that the CCPA need not regulate data that is already protected under other regulatory regimes. Second, the legislature appreciates that the critical societal benefit that flows from the collection and use of certain data, including information collected as part of a medical clinical trial, may in certain circumstances outweigh an individual's right to fully control what happens with that data.⁶

However, as detailed in this letter, we have identified certain CCPA language that requires clarification to ensure that this apparent legislative intent is honored. For example, the CCPA's HIPAA exemption extends to certain data collected by HIPAA "covered entities" and "business associates," designations that in most cases do not apply to Genentech.⁷ As a practical matter, HIPAA covered entities often transmit coded health information to Genentech as authorized under applicable law and upon obtaining patient consent and authorization. Such data is typically labeled with a specific code and does not carry any personal identifiers. The providing party is responsible for maintaining the coding key. This coding is the current standard used in clinical research, including observational studies, and offers additional privacy safeguards to the individual. Before any sharing of such received information, it is further de-identified by Genentech in accordance with applicable privacy laws⁸ so that associating the data with any particular individual is unfeasible. Regardless of such de-identification, Genentech securely handles the information in a lawful and appropriate manner, including through systems and processes, such as encryption, system security, internal access restrictions, and other safeguarding protocols. Although Genentech holds this information in compliance with existing applicable privacy laws and standards, the information is not clearly exempt from the CCPA.

⁶ California Civil Code § 1798.145(c)(1)(C). Under HIPAA, information collected for treatment, payment, or health care operations may generally be de-identified (in accordance with specified standards) and used for secondary purposes without a patient authorization, including research. Additionally, the EU Data Protection Board opined that the use of data for secondary research is legitimate under the GDPR so long as companies implement appropriate safeguards such that a new legal basis need not be established.

⁷Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in certain transactions. Business Associate is a person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information.⁸ HIPAA, the CMIA, or the GDPR, as applicable.

⁸ HIPAA, the CMIA, or the GDPR, as applicable.

We are concerned that, as enacted, the CCPA could create unintended barriers to scientific, healthcare related work in the public interest and inhibit otherwise appropriate use of health information to advance science and medicine and enable patient access to necessary treatments. We therefore propose the following recommendations for your consideration, which we believe are within the Attorney General’s rulemaking authority, are consistent with legislative intent, and address our identified issues.

I. Priority Issues and Proposed Resolutions.

1. Clinical Trial Exemption and Related Research

Clinical trial research is a central component of Genentech’s operations. As of January 2019, Genentech and other Roche group companies have conducted 773 trials involving nearly 35,000 patients in over 3,000 locations across California. As amended, the CCPA exemption for collected clinical trial data remains ambiguous regarding what research standards must be followed to qualify for the exemption.⁹ We request that regulations state “clinical trial data is exempt if the research is conducted pursuant to *any* of: (a) the federal Common Rule,¹⁰ (b) the ICH GCP standards,¹¹ or (c) FDA human subject protection standards”¹².

In addition, we propose a regulatory safe harbor for other clinical or human subject research that satisfies *any* of the following, so long as study data is protected under current privacy standards (e.g. coding, pseudonymization, anonymization or de-identification):¹³ (d) if approved or granted waiver by an independent review board (“IRB”) or is exempt from such IRB approval, (e) if approved or granted waiver by an ethics committee, or (f) if conducted pursuant to Good Pharmacoepidemiological Practices, or other accepted industry practice guidelines.

Further, we suggest clarifying that information collected “as part of” a clinical trial includes “any information collected or created (including, without limitation, biospecimens, biometrics, and images), that reasonably relates to, or in any way furthers the purpose of, the conduct of any present or prior qualifying clinical trial or clinical or human subject research.”

We propose the above clarifications in the rulemaking process for the following reasons. First, certain CCPA commenters have suggested that the clinical trial exemption language could be interpreted to exempt clinical trial data *only if* it is subject to the federal “Common Rule” (along with other standards), an interpretation that may fail to exempt important privately funded research that is subject to other existing data privacy standards and research controls.

Second, we recommend a regulatory safe harbor for other healthcare-related research and development by private businesses, including research performed *outside* the clinical trial

⁹ See California Civil Code § 1798.145(c)(1)(C).

¹⁰ Title 45 of the Code of Federal Regulations Part 46.

¹¹ International Council for Harmonisation Good Clinical Practice guidelines.

¹² United States Food and Drug Administration human subject protection requirements (Title 21 of the Code of Federal Regulations Parts 50 and 56 .

¹³ Current privacy standards under HIPAA, the CMIA , and the GDPR.

context, to acknowledge the public health benefits that flow from such research. We request that these research methods be deemed compliant with the CCPA when conducted in accordance with current applicable privacy laws and recognized industry practice guidelines.¹⁴ Although companies generate such research data outside of clinical trials, the research and resulting data promote similar public health benefits, potentially inviting insights and breakthroughs that may otherwise elude alternative research techniques.¹⁵ This research safe harbor would be consistent with the legislature's apparent intent in establishing the clinical trials exemption, by creating a safe harbor for other types of healthcare research conducted in accordance with other recognized research guidelines and standards,¹⁶ and with resulting data protected under current privacy standards, such as de-identification, anonymization, and pseudonymization.¹⁷

Finally, we note that the CCPA clinical trial exemption does not define or otherwise clarify the phrase "as part of." For example, we are uncertain whether certain secondary research data is exempt under the CCPA, when a company previously collected the data used for such secondary research "as part of" a prior clinical trial in accordance with current applicable laws. Similar questions arise regarding repository biological samples which are not used contemporaneously with a given clinical trial. For those reasons, we recommend the clarifying regulation discussed above.

2. "Consumer" Definition

Although the CCPA applies to California "consumers," this definition is not limited to consumers *in the traditional sense*. Instead, the law broadly defines the term as any "natural person who is a California resident . . . however identified."¹⁸ We propose that regulations clarify this definition to mean "a California resident who uses a product or service *in a personal capacity*." Additionally, we propose that implementing regulations exclude from the "consumer" definition any individuals acting in their capacity as employees, service providers, professionals, or *any other representatives* whose engagement with a business derives from a business-to-business relationship.

As enacted, certain business representatives with whom a company engages are likely considered "consumers" under present CCPA language, including representatives of vendors, healthcare providers, and health plans. Without clarification, it is unclear how a company like Genentech

¹⁴ Such research, which is often performed by private parties, involves the collection of medical information where consistent with informed consent, including, without limitation, patient reported data, information gathered from monitoring devices, and electronic health records.

¹⁵ For example, outside research may involve software and the utilization of machine learning in attempting to identify patterns and insights that may otherwise be unidentifiable. The research may also reduce the need for interventional trials and provide significant benefits such as answering research questions, helping with clinical trial design, supporting drug product label expansion, informing payer questions, supporting post-marketing follow-up, and improving knowledge of disease, biology, and individual health.

¹⁶ Examples include, without limitation, IRB review or exemption, Good Pharmacoepidemiology Practices, EMA Good Pharmacovigilance Practices Guidelines, and National Institutes of Health guidelines.

¹⁷ Current privacy standards under HIPAA, the CMIA, and the GDPR.

¹⁸ California Civil Code § 1798.140(g)(emphasis added).

would comply with the CCPA in the case of an employee, vendor representative, or individual healthcare provider who is *also* the company's end-consumer in the traditional sense. In this situation, fulfilling a CCPA request to *delete* information may have unintended consequences. For example, a healthcare provider may invoke CCPA consumer rights to request deletion of his or her personal health information such as diagnosis or test results, and CCPA compliance may require removing all such information on record for the healthcare provider's business entity (potentially including information of more than one individual). For these reasons, we recommend that regulations clarify the definition of "consumer."

3. "Personal Information" Definition

CCPA's broad definition of "personal information" includes information 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*.¹⁹ This definition includes identifiers which, taken together, create a more expansive and ambiguous standard than other privacy laws, and may relate to more than one individual.

Consistent with existing privacy laws, we propose that regulations clarify the definition of "personal information" and any identifiers to be specific to a *single individual*, as follows (a) the phrase "a particular consumer or household" refer to an identifiable individual residing at a specific California postal address, excluding any spouse, dependents or others, regardless of household affiliation, and (b) an identifiable consumer be someone identified by name or specific identifiers *by the business collecting such information*, without requiring additional investigational efforts. Also, we propose a regulatory safe harbor clarifying that companies are *not* required to link or re-identify consumer data to satisfy CCPA requirements²⁰ when following current privacy and data protection standards of de-identification, anonymization, or pseudonymization of personal information, as authorized under applicable laws,²¹ and that such privacy standards be recognized as satisfying privacy protection of personal information for CCPA compliance.

Genentech in many circumstances has no way to verify a unique individual based on IP addresses or device IDs, or based on coded (or pseudonymized) information, without receiving other personal information or being required to "re-link" information that had previously been un-linked (or never received) to protect an individual's privacy. Regulatory clarification is needed so that investigative efforts of this type, which are contrary to current privacy practices, are not required to comply with CCPA.

¹⁹ California Civil Code § 1798.140(o)(1)(emphasis added).

²⁰ In making this point, we acknowledge one CCPA exemption indicating that businesses need not "link information" under certain circumstances; however, without further guidance, it is unclear how a company could qualify for this exemption. See California Civil Code § 1798.145(i).

²¹ HIPAA, the CMIA, or the GDPR, as applicable.

We also note that responding to certain CCPA “personal information” requests, such as deleting or disclosing certain information, may necessitate that Genentech re-identify an individual and link data when an individual would otherwise remain unidentified following current privacy standards. In practice, extracting a single individual’s data *from coded or de-identified datasets* is often not practical, in many instances not readily possible, and could stifle important research objectives.²² Any of the foregoing circumstances would likely involve the unintended collection or use by Genentech of more identifiable information than would have been necessary absent the consumer request, resulting in a net loss in privacy to the individual.

4. “Sale” Definition

The CCPA broadly defines “sell, selling, sale, or sold” to include selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal information to another business or third party for monetary *or other valuable consideration*.²³ As written, this definition implicates several activities beyond mere “sales” in the traditional sense. Further, the CCPA requires that any covered business that “sells” personal information to third parties must provide notice to consumers of such sales, and CCPA consumers have the right to “opt-out” of those sales.

We propose that implementing regulations state that “valuable consideration” means the exchange of data for cash or direct commercial gain, and specifically excludes *any transaction for research or development purposes* that makes available, exchanges, or transfers data (whether or not for limited periods and subject in all cases to applicable existing privacy protection standards for data sharing), even where valuable consideration may be provided in such transaction. This clarification in the regulations is necessary to give assurance that biopharmaceutical and life science companies are permitted under to continue to use privacy-protected data to combine with or link to other data and be used for research purposes, to advance science and public health, or for analysis, development, and commercialization of products to treat and diagnose disease.

“Sale” language should align closely with general consumer understanding, so that consumers fully understand the consequences of their “opt-out” decisions. We also recommend permitting biopharmaceutical companies to explain the various types of sales and allow consumers the choice to opt-out of any *portion* of these types of sales, depending upon indicated business use.

There are several reasons prompting these recommendations. For example, we believe it is critical to allow consumers to designate the sale types for any CCPA opt-out requirement. This is

²² *Illustrative Example*: Genentech continuously conducts retrospective analyses on de-identified patients to understand, for example, optimal treatment patterns and points of intervention to optimize patient outcomes and experience. The CCPA’s application may result in the need to “semi-identify” the data, to remove California residents, which would disrupt Genentech’s work analyzing large de-identified datasets across a comprehensive sample set, despite underlying intentions of advancing patient care. Such data removal might also inadvertently introduce bias or otherwise distort research results.

²³ California Civil Code § 1798.140(t).

because Genentech offers individuals the opportunity to opt-in and consent to use of their information in order to receive a variety of benefits and services, such as nurse telephone calls and medication access services. Without clarification of the CCPA “opt-out” requirement, an individual’s opt-out decision could unintentionally terminate these important services. Genentech also engages third parties to provide coupons, co-pay cards, medical education, and medication adherence programs, each of which require individual information disclosures to third parties that could feasibly fall under the definition of “sale.” Without implementing our recommendations regarding the “sale” definition and individual choice for a partial “opt-out,” a consumer’s opt-out request may unintentionally impede these critical data sharing practices.

Further, Genentech’s third party data sharing practices are critical to improving research and personalized patient care. Examples of such arrangements include global data collaboration among researchers,²⁴ the transfer of patient tissue in connection with individualized cancer treatments,²⁵ and data purchased from genomics companies to further research initiatives.

II. Additional CCPA Concerns.

In addition to the above described priority issues, Genentech notes the following additional issues with the CCPA that we believe warrant rulemaking consideration:

1. Look-Back Time Periods and Implications. A shortened compliance timeline exacerbates the resource intensive challenges associated with data protection compliance, particularly as businesses await implementing regulations and other guidance. We are particularly concerned regarding whether the 12-month lookback period might cause the CCPA compliance period to begin prematurely. We propose that businesses be given no less than 9 months to bring their organization into

²⁴ *Illustrative Example:* One Company policy requires sharing individual level clinical trial data with other researchers to use for their legitimate research questions under a research plan and under appropriate and compliant data protection conditions. Such sharing may occur on an international scale. The relevant data sharing agreement restricts using data beyond the researcher’s identified research plan, restricts the sharing of that data with others, and prohibits attempts to re-identify data subjects. Additionally, the researcher is requested to publish findings, which could serve to further additional research on similar issues, ultimately bestowing a supreme benefit to public health. Under the CCPA, this type of research sharing could be considered a “sale,” triggering several data rights for data subjects. Because Genentech does not receive direct identifiers, however, the company has no way of knowing the identity of individuals to be able to comply with the CCPA without further identification efforts. The administrative cost and effort to track the research use of an individual’s data could cause the company to restrict or discontinue such broad clinical trial sharing programs, despite intentions to advance science, medicine, and public health globally.

²⁵ *Illustrative Example:* One innovative Genentech program creates individualized treatments for cancer patients. This requires the transfer of patient tissue to a healthcare provider and then to a Genentech partner, which sequences the patient’s DNA. The resulting DNA sequencing data must be transferred once more for analysis. The results of that analysis are then transferred back to Genentech and used to manufacture the individualized treatment, as well as for additional research and improvements to the treatment. It is unclear whether any of these transfers would constitute a “sale” under the CCPA. In the process of analyzing this information and creating data, some or all of these partners would likely use the data to improve their own processes and capabilities, which may or may not constitute “valuable consideration” under the CCPA. This lack of clarity could negatively impact the creation and improvement of important medicines that treat unmet medical needs.

compliance after final regulations are published, and that the CCPA should apply only to personal information collected or disclosed after the effective date of the law.

2. "Homepage" Definition. The CCPA defines "homepage" to include the introductory page of a website, but also potentially *any* web page "where personal information is collected." Genentech recommends clarifying that the definition's "introductory page" language applies to the "homepage" definition universally, rather than imposing certain CCPA homepage requirements for *any* web page where personal information is collected.
3. Data Security Program Safe Harbor. The CCPA's consumer private right of action enforcement mechanism should include a safe harbor for businesses that have implemented a data security program that is reasonable and consistent with recognized industry standards.


Genentech remains committed to collecting and using personal data in a lawful, fair, and responsible manner. We are also committed to advancing the public's interest in science and medicine and access to healthcare, which increasingly depends on the collection and use of personalized healthcare data. We are therefore grateful for your efforts in soliciting public input early in the rulemaking process. We would be happy to meet or discuss the contents of this letter at your convenience, to follow up with specific language proposals to address our concerns, and, if welcome, to work with your staff on regulation wording.

Very truly yours,

GENENTECH, INC.



Sean A. Johnston
Senior Vice President
General Counsel and Chief Compliance Officer

cc: Ms. Amy Zajac
Genentech Government Affairs


Message

From: Dwyer, Patrick [REDACTED]
Sent: 5/1/2019 10:08:44 AM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: RE: California Consumer Privacy Act of 2018—Pre-Rulemaking Comment Letter
Attachments: Comments on CA Consumer Privacy Act.pdf

Dear Sir or Madam:

Mastercard International Incorporated appreciates this opportunity to submit written comments in response to the preliminary rulemaking activities undertaken by the California Department of Justice prior to the official rulemaking required by the California Consumer Privacy Act of 2018.

Best,

Patrick Dwyer

Patrick Dwyer
Director
State Public Policy

Mastercard | mobile [REDACTED]



CONFIDENTIALITY NOTICE This e-mail message and any attachments are only for the use of the intended recipient and may contain information that is privileged, confidential or exempt from disclosure under applicable law. If you are not the intended recipient, any disclosure, distribution or other use of this e-mail message or attachments is prohibited. If you have received this e-mail message in error, please delete and notify the sender immediately. Thank you.

April 30, 2019

By Email

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act of 2018—Pre-Rulemaking Comment Letter

Dear Sir or Madam:

Mastercard International Incorporated (“Mastercard”)¹ appreciates this opportunity to submit written comments in response to the preliminary rulemaking activities undertaken by the California Department of Justice prior to the official rulemaking required by the California Consumer Privacy Act of 2018 (“CCPA” or the “Act”).

Discussion

A. Introduction

The CCPA requires that on or before July 1, 2020, the Attorney General (“AG”) solicit broad public participation to adopt regulations implementing the CCPA. Cal. Civ. Code § 1798.185(a). The CCPA specifically requires the AG to solicit public participation and adopt regulations to further the purposes of the CCPA with regard to seven enumerated areas. Id. Mastercard’s comments are focused on two topics in areas for which the AG is required to solicit public participation and issue regulations as needed: what should (and should not) be included in personal information, id. § 1798.185(a)(1), and exceptions to the Act’s coverage to comply with state or federal law relating to trade secrets and intellectual property rights. Id. § 1798.185(a)(3).

Accordingly, as your office prepares to issue regulations in accordance with the CCPA, we respectfully submit the following requests for clarification for your consideration. Mastercard believes these clarifications will better enable all interested parties to comply with

¹ Mastercard is a technology company in the global payments industry. We operate the world’s fastest payments processing network, connecting consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. Mastercard’s products and solutions make everyday commerce activities—such as shopping, traveling, running a business and managing finances—easier, more secure and more efficient for everyone.

the law, provide needed certainty with regard to legally protected proprietary interests, and ensure consistency with the intent of the CCPA.

B. Definition of “Personal Information”

The CCPA requires the AG to solicit public input and issue regulations as needed on what information should be included in personal information. Cal. Civ. Code § 1798.185(a)(1). How personal information is ultimately defined is a key issue under the Act, because the Act establishes various rights of consumers with respect to their personal information that is collected or held by businesses. Similarly, for businesses, the definition of personal information is significant because it defines the scope of the obligations of businesses that collect or hold personal information about consumers. The definition of personal information in the Act includes several vague phrases that do not appear to have been used in a U.S. or major international privacy law, including, for example, the phrase “capable of being associated with.” Cal. Civ. Code § 1798.140(o)(1). Such novel and vague language is potentially unlimited in its breadth, which will create significant uncertainty as to the scope of consumer rights and the impact and obligations from the CCPA on businesses. Thus, Mastercard believes that it is important to ensure that the question of what is included, and necessarily what is not included, in the definition of personal information is clear.

In this regard, Mastercard respectfully suggests that the rules issued by the AG should make clear that “personal information” does not include pseudonymous information. Mastercard believes that the exclusion of pseudonymous information from “personal information” is consistent with both the language of the Act and its intent.

For example, the CCPA defines “personal information” to mean “information 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.” Cal. Civ. Code § 1798.140(o)(1). The definition includes a list of eleven types of information that may constitute personal information, including “identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers[.]” but in each case such information falls within the definition only “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[.]” *Id.* While this definition is broad, the Act also recognizes privacy protective data minimization processing by including explicit references and definitions for “deidentified,” “aggregate consumer information” and “pseudonymize” or “pseudonymization.” *Id.*, at § 1798.140(a), (h) and (r).

Consistent with the basic definition of personal information, the Act defines “pseudonymize” as “the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.” Cal. Civ. Code § 1798.140(r).

Once information is pseudonymized, a business that holds such information should have no obligation to re-link or reidentify the information data that has been disassociated with and is no longer attributable to a particular consumer in order to satisfy a request by a consumer wishing to exercise their rights under the Act. For example, the CCPA provision that entitles a consumer to request that a business disclose personal information that the business has collected about the consumer states explicitly that “this section shall 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.” Cal. Civ. Code § 1798.100(e). Similarly, the CCPA section that lists the information that a business must disclose to a consumer states that the business is not required to “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.” Cal. Civ. Code § 1798.110(d)(2). Finally, the CCPA contains a general statement of intent making clear that “this title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.” Cal. Civ. Code § 1798.145(i).

Given the existing definitions of “personal information” and “pseudonymize” and the fact that the Act is clear that a business has no obligation to reidentify information, Mastercard believes that the intent of the Act is not to treat pseudonymized information as personal information. However, the Act contains provisions that could create some confusion, which is why Mastercard believes clarification is necessary. In particular, the definition of personal information includes numerous traditional identifiers, as well as “other similar identifiers.” Cal. Civ. Code § 1798.140(o)(1)(A). This creates potential ambiguity for pseudonymized data sets which replace attributable identifiers with anonymous identifiers. To avoid confusion, Mastercard respectfully suggests that the AG clarify this point in its rules implementing the Act by expressly stating that pseudonymized information does not constitute personal information, or that a pseudonymized identifier is not an identifier per Cal. Civ. Code § 1798.140(o)(1)(A).

C. Application of the CCPA to Intellectual Property or the Disclosure of Information that would Reveal Data or Infringe on a Third Party’s Rights

The CCPA specifically grants the AG the authority to establish “any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.” Cal. Civ. Code § 1798.185(a)(3).

Federal and state laws provide a variety of protections for intellectual property, including information subject to copyright, patent, service mark and/or trade secret protections. In addition, many businesses hold information the disclosure of which would infringe or adversely effect the rights or freedoms of third parties. Mastercard respectfully suggests that the AG, under the authority noted above, issue rules establishing an exception from the CCPA’s access and deletion obligations for those types of proprietary information that are subject to protection under federal or state law. Mastercard respectfully suggests that a business should not be required to disclose or delete any information that is subject to intellectual property protections, including any formula, pattern, compilation, program, device, method, technique, or process

developed to process or analyze personal information, any information derived from such process or analysis, or any other trade secrets, intellectual property or material nonpublic information.

D. Conclusions

Mastercard appreciates the opportunity to provide comments regarding the preliminary rulemaking required by the CCPA. If there are any questions regarding our comments, please do not hesitate to contact the undersigned at [REDACTED] or [REDACTED], or our counsel at Sidley Austin LLP in this matter, Joel D. Feinberg, at [REDACTED]

Sincerely,

/s/ Patrick S. Dwyer

Patrick S. Dwyer
Director, Public Policy, U.S. Markets

cc: Joel D. Feinberg, Sidley Austin LLP
Patrick K. O'Keefe, Sidley Austin LLP



May 29, 2019

The Honorable Ed Chau
Chair
Assembly Privacy & Consumer Protection Committee
Room 156A, Legislative Office Building
1020 N Street
Sacramento, CA 95814

The Honorable Hannah-Beth Jackson
Chair
Senate Judiciary Committee
State Capitol, Room 2187
Sacramento, CA 95814

RE: CALIFORNIA CONSUMER PRIVACY ACT – COMMENT LETTER

Dear Chairs Chau and Jackson,

On behalf of the Orange County Business Council (OCBC), representing the interests of over 200 businesses throughout Orange County, I am writing to share our very significant concerns about the potential impacts of the California Consumer Privacy Act (CCPA). **OCBC absolutely supports consumer privacy, but we must ensure that our laws are realistic and do not unduly inhibit commerce.**

Orange County is thriving. As the sixth largest county by population in the nation, Orange County is experiencing record levels of unemployment at 2.8 percent and falling, a higher educational attainment rate than peer regions, and an economy of over \$19.2 billion from emerging S.T.E.A.M. (Science, Technology, Engineering, ARTS, and Mathematics) industry clusters in the region alone. Orange County is a success story—having succeeded by capitalizing on the high-octane mix of capital, skilled labor and creative forward-thinking that has drawn artists and entrepreneurs alike to its shores for over a century. Legislative actions should protect this engine of growth, not harm it.

CCPA was passed quickly and we are now facing an urgent need to resolve open questions and address unintended consequences. Failure to do so could undermine the ability of our businesses to communicate with their customers, or make it much for difficult or expensive market their products and services. They could also face new costs for compliance and threats of litigation, despite good faith efforts to protect consumer data. Clearly, there is much work to be done in the way of establishing definitions, thresholds, rules, procedures, exceptions, etc. to make the CCPA law understandable, workable, and enforceable.

We strongly encourage the Attorney General and Legislature to work with the business community throughout the legislative and rulemaking processes to seek amendments to CCPA and establish reasonable regulations that protect privacy while giving consideration for the added costs and burdens placed on businesses to comply.

Specifically, OCBC is supportive of the proposals outlined in AB 873 (Irwin), which would appropriately clarify the definition of “personal information” and relieve small businesses from costly and time-consuming actions to unnecessary organize, re-identify and store customer information in way that is counter to the goals of consumer privacy. We also encourage

support for AB 846 (Burke), which will preserve the ability of businesses to offer loyalty programs, and AB 1564 (Berman), which allows for an email option for how consumers can request their personal information from a business under CCPA – not just an outdated 1-800 number system. Additionally, we support SB 753 (Stern) that would clarify the definition of “sale of information” as it relates to advertising. This is critically important to businesses trying to build awareness of their products or services among existing and potential customers.

Consumer privacy issues are complicated. But it's important that policymakers take the time to get this right. The Silicon Valley tech titans may have vast resources to hire teams of lawyers, but most of our member companies in Orange County are simply trying to run their businesses responsibly and profitably, and don't have the same level of resources. It is crucial that lawmakers fix CCPA's provisions now to protect small businesses before it takes effect in 2020. Failure to do so will inhibit operations and growth for businesses large and small, create costly barriers to online business tools, impose ambiguous restrictions, create uncertainty and discourage innovation.

Thank you for your consideration of these issues as you review new legislative proposals to modify and improve consumer privacy rules in California.

Sincerely,



Alicia Berhow
Senior Vice President of Government Affairs

cc: The Honorable Tom Umberg, State Senator, 34th District
The Honorable Xavier Becerra, California Attorney General

Message

From: Burstein, Aaron [REDACTED]
Sent: 5/17/2019 5:40:09 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: CCPA Rulemaking -- Comments of BSA
Attachments: BSA CA AG Rulemaking Comments FINAL-c1.pdf

Please see the attached comments of BSA | The Software Alliance on regulations to implement the California Consumer Privacy Act. Please do not hesitate to contact me if you have any questions.

WILKINSON) BARKER) KNAUER) LLP

AARON J. BURSTEIN
PARTNER
1800 M STREET, NW
SUITE 800N
WASHINGTON, DC 20036



WWW.WBKLaw.COM

NOT ADMITTED IN DC; PRACTICE LIMITED TO FEDERAL AGENCIES

Comments of BSA | The Software Alliance on Regulations to Implement the California Consumer Privacy Act

BSA | The Software Alliance (“BSA”) respectfully submits these comments on the development of regulations to implement the California Consumer Privacy Act (“CCPA” or “Act”). BSA is the leading advocate for the global software industry in the United States and around the world.¹ Our members are at the forefront of developing cutting-edge, data-driven services that have a significant impact on US job creation and the global economy. BSA members prioritize protecting the privacy and security of their customers’ personal information. BSA strongly supports efforts to ensure a robust US privacy framework that provides increased transparency, enhances consumers’ control over their personal information, safeguards their data, and enables legitimate uses of data that fuel continued innovation. We appreciate California’s leadership on these important issues.

The CCPA and its regulations should maintain a strong set of privacy protection for California consumers, and thoughtfully crafted regulations that address some of the practical difficulties in implementing the law are an important means of achieving this goal. Importantly, many BSA members primarily provide services to business customers, and practical interpretations of the law that continue to distinguish between the role that a “business” and “service provider” play will help different organizations across the data ecosystem understand and implement appropriate obligations to protect consumers’ privacy. These comments identify several challenges that arise from ambiguities in the CCPA’s text but could be clarified through regulations. BSA’s proposed clarifications would not only provide certainty for companies that must comply but also would help to establish practices that are consistent with consumers’ expectations and the CCPA’s purpose of strengthening consumer privacy protections. Specifically, BSA recommends that the Attorney General issue regulations that would:

- Clarify the scope of “personal information”;
- Clarify that the definition of “consumer” does not apply to employees;
- Help ensure that opt-out requests are meaningful to consumers; and
- Provide guidance on consumer verification methods and responses to consumer requests.

We recognize that the legislative process to amend the CCPA is ongoing, and there are several bills under consideration that may address—at least in part—some of these issues. However, there is continued uncertainty regarding what the outcome of those deliberations will be and, in some instances, current proposals are not sufficiently comprehensive to address more granular implementation details under review by the Attorney General’s office. As a result, we respectfully request your consideration of these important issues.

I. Clarify the Scope of “Personal Information” in Connection with Households and Publicly Available Information.

The CCPA provides an exceptionally broad definition of “personal information.”² BSA requests that the Attorney General address two elements of the definition that present significant difficulties from an implementation perspective.

¹ BSA’s members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

² See Cal. Civ. Code § 1798.140(o).

A. Limit Obligations Concerning Household Information.

One set of challenges stems from including information about households in the CCPA's definition of "personal information."³ Although the CCPA does not define "household," the term could encompass, for example, spouses, children, and roommates who share a dwelling. The purpose of considering household information to be "personal" may have been to deem Internet Protocol addresses and information associated with them to be personal information – which is something the definition does anyway.⁴ This aspect of the "personal information" definition is out of step with other privacy laws and will create negative consequences for consumers and their privacy.

Specifically, it is unclear whether the right to opt out of sale applies to information about a household, rather than being limited to information about the specific consumer who makes an opt-out request. Section 1798.120 gives consumers the right to "direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information." The use of "the consumer's" to modify personal information, however, suggests that this right is also limited to information about the consumer who makes a request.

Leaving open contrary interpretations, *i.e.*, that household-level information is subject to the right to opt out of sale, would have negative consequences for consumers' privacy as well as business that must obey opt-out requests. For instance, roommates who are part of the same "household" might have quite different preferences about whether or not they want to prevent the sale of personal information. Similarly, parents might make different choices about the sale of their personal information than they make for their children.⁵ If decisions about the sale of personal information apply to information that relates to an entire household, it is unclear how businesses will be able to maintain different individuals' preferences. Further, disclosure of information pertaining to other household members in connection with access and deletion requests could undermine the privacy rights of other consumers.

To address these difficulties, the Attorney General should adopt regulations clarifying that the right to opt out of sale applies only to information about the specific consumer who makes an opt-out request. In addition, BSA recommends that the Attorney General's regulations permit businesses to take reasonable measures to maintain individual-level opt-out preferences and to forbear from disclosing or deleting personal information, as necessary, to avoid implicating information that is about a household member, rather than an individual making a request.

B. Recognize That the Government's Disclosure of Personal Information Entails the Purpose of Further Dissemination and Use.

The second significant difficulty that the Attorney General could address concerns the exclusion of "publicly available" information from the definition of "personal information."⁶ The exclusion is an important element of the CCPA,⁷ but, unfortunately, it is beset by a lack of clarity. Under section 140(o)(2), information is "publicly available" if it "is lawfully made available from federal, state, or local government records, if any conditions associated with such information." Publicly available information, however, excludes "data [that] is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained."

³ See *id.* § 140(o)(1).

⁴ See *id.* § 140(o)(1)(A) (defining "Internet Protocol address" and "other similar identifiers" to be "personal information").

⁵ See Cal. Civ. Code §1798.120(c) (requiring opt-in consent to sell information about consumers under the age of 16).

⁶ See Cal. Civ. Code § 1798.140(o)(2) ("Personal information" does not include publicly available information.).

⁷ See *id.*

Thus, the publicly available information exemption apparently requires businesses to ascertain the purpose, or purposes, for which government agencies maintain and release personal information. Releases of personal information by government agencies may have multiple purposes, not all of which are clear. In many cases, however, agencies release information in order to provide transparency and accountability through further analysis, for example, by journalists and researchers. Making businesses responsible for determining the purposes for which the government publishes information is inconsistent with the basic notion of making information publicly available in the first place.

The Attorney General should clarify that, for the purposes of the CCPA, a government agency's decision to make information available to the public demonstrates a purpose of allowing others to make use of the information for any lawful purpose. Such a regulation would be consistent with the CCPA's text as well as the broad purposes behind government policies of making information available to the public.

II. Limit CCPA Obligations as Applied to Employees.

A focus on *consumer* privacy pervades the CCPA. "Consumers" and "businesses" are fundamental terms in the Act, which does not refer to "employees" or "employers" at all. Nonetheless, the CCPA does not expressly exclude employees⁸ from the definition of "consumer,"⁹ and the definition of "personal information" includes "professional or employment-related information."¹⁰ Thus, the CCPA's text suggests that employees and personal information relating to individuals acting in their capacities as employees are covered by the Act, notwithstanding that the overarching aim of the law is to protect "consumer" privacy.

If the CCPA is interpreted to include employees, many of the documents that employers routinely collect would be subject to the full array of consumer rights. These documents include CVs and resumes, evaluation and disciplinary records, payroll and tax record information, vacation and sick leave balances, and health plan and other benefits documentation. Such an interpretation will create several significant operational challenges for a wide range of businesses and employees while doing little, if anything, to promote *consumer* privacy. Some of the challenges include the following:

- *Right to Delete.* Employers need to keep employee data for payroll, to administer benefits, to guard against legal claims, and for myriad other management purposes. If a deletion request from a consumer requires the business to delete all information about that consumer in his or her capacity as an employee of the business, those functions could become impossible to administer.

Although the CCPA provides several exceptions to the right to delete, these exceptions do not cover the full range of legitimate processing by an employer, and the catch-all exception for use "in a lawful manner that is compatible with the context in which the consumer provided the information"¹¹ does not sufficiently clarify that an employer could reject a deletion request.

- *Right to Opt Out of Sale.* The right to opt out of sale of personal information is incongruous in the employment setting. Although most employers do not sell employee data in the commonly

⁸ This comment uses "employee" to refer to an individual acting in an employment- or business-related capacity, including as an employee, contractors, job applicant, director, officer, or agent of a business.

⁹ See Cal. Civ. Code § 1798.140(g). Section 1798.140(g), in turn, refers to Cal. Code of Regulations, title 18, section 17014, which defines resident to "include (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose." This definition is expansive and appears to mean that any natural person with the requisite ties to California is a consumer, regardless of the nature of his or her interaction with the entity collecting and processing his or her personal information.

¹⁰ Cal. Civ. Code § 1798.140(o)(1)(I).

¹¹ Cal. Civ. Code § 1798.105(d)(9).

understood meaning of that word, the CCPA's broad definition of "sell" could potentially create situations where an employer's legitimate use of an employee's data could be considered a sale under the CCPA. In the absence of clarification from the Attorney General, employers will need to scrutinize each instance in which they provide data to a vendor, such as a payroll processor, and may need to seek to modify their contracts with vendors to avoid the result where the vendor's processing could be considered a sale. These changes will add to the CCPA's compliance costs.

- **Access.** The right of a consumer to obtain personal information that a business "has collected about that consumer"¹² also presents challenges for employers. For example, employee information could be particularly sensitive during mergers or planning for personnel changes. The narrow exceptions that the CCPA provides to the access right are likely insufficient to address these and other situations that require employers to keep employment records confidential.

BSA therefore recommends that the Attorney General clarify that employees are not "consumers" under the CCPA. In so doing, it would provide certainty to businesses and their vendors, reduce compliance costs, and prevent the CCPA's consumer rights from becoming unintended means of compromising the confidentiality of employee records or deleting them altogether. Notwithstanding the clear intent of the CCPA to address consumer privacy and the overwhelming policy reasons for excluding employees from the scope of the law, if the Attorney General interprets the CCPA to cover the employment context, we request consideration of alternative mechanisms for deletion, access, and opt-out requests that apply to employees to mitigate the harmful consequences, such as those referenced above, that could arise.

III. Ensure That Opt-Out Requests Are Helpful and Meaningful to Consumers.

A. Allow Granular Opt-Out Requests.

The opt-out right under the CCPA sweeps broadly. The CCPA directs businesses to provide a means (further discussed below) allowing consumers simply "to opt-out of the sale of the consumer's personal information."¹³ In many circumstances, consumers might wish to opt out of some sales of personal information while allowing others to continue, rather than making an all-or-nothing choice. Allowing businesses to present granular choices to consumers would help to avoid some of these potential consequences.

BSA recommends that the Attorney General clarify that the CCPA allows businesses to give consumers the choice to opt out of certain types of sales and does not require businesses to present all-or-nothing choices. This clarification would give businesses the flexibility to tailor opt-out choices that meet customers' expectations and provide them with greater control over their personal information.

B. Provide Flexibility for Opt-Out Link Displays.

Some of the CCPA's requirements for a "Do Not Sell My Personal Information" link may be difficult to satisfy in practice. Specifically, the CCPA requires this link to appear clearly and conspicuously on the "homepage" and in the privacy policies of businesses that sell personal information.¹⁴ The definition of "homepage," in turn, refers to the term "online service," which is not defined and could capture a wide range of services, potentially including some businesses that do not have a consumer-

¹² Cal. Civ. Code §§ 1798.110(a)(5), (c)(5). *See also id.* § 1798.100(a).

¹³ Cal. Civ. Code § 1798.135(a)(1); *see also id.* § 1798.120

¹⁴ *See* Cal. Civ. Code §§ 1798.135(a)(1), (2); *see also id.* § 1798.140(l) (defining "homepage").

facing presence.¹⁵ However, it may be difficult for non-consumer-facing services to satisfy all of the opt-out link standards that apply to “online services.” For example, it is unclear how a company that does not provide a mobile app or other service that consumers use would meet a requirement to provide the opt-out link “before downloading the [business’s] application.”¹⁶

A separate issue is that the definition of “homepage” appears to require companies to display an opt-out link on every page on which personal information is collected.¹⁷ Requiring the opt-out link to become effectively ubiquitous could lead to “notice fatigue” where consumers ignore it altogether, which undermines the consumer right that the CCPA provides.

To address these challenges, BSA recommends that the Attorney General issue regulations clarifying the obligations of businesses that do not have direct relationships with consumers regarding the opt-out link.¹⁸ These regulations could, for example, clarify that an “online service” is one that is directed to consumers and provide that it is sufficient for businesses that are not consumer-facing to disclose a point of contact to address consumers’ questions and provide a link to their privacy policies or other educational materials. With respect to placement of the opt-out link, the Attorney General should consider regulations that give businesses the flexibility to place the link in locations in which consumers are likely to find it, based on the nature of their services and how consumers use them.

C. Provide Guidance on Consumer Verification Methods and Responses to Consumer Requests.

Implementation of the CCPA’s verifiable consumer request requirements must balance several objectives. On one hand, it should be easy for consumers to make access, deletion, and opt-out requests.¹⁹ On the other hand, the inadvertent deletion or disclosure of personal information to someone other than the consumer presents a wide range of risks; consumer verification methods should provide adequate safeguards against these risks and should not require businesses to collect and process sensitive personal information solely to support verification.²⁰ Moreover, verification methods must be reasonable in light of the sensitivity of the information at issue, the capabilities of available technologies, and the costs to implement them.²¹

Businesses will also confront the challenge of responding to consumers who cannot be verified. Although the CCPA does not require a business to provide access to or delete personal information when the business cannot verify a consumer,²² it does not provide further detail about the form that a response should take in such a situation.

¹⁵ See Cal. Civ. Code §1798.140(l).

¹⁶ See *id.*

¹⁷ See Cal. Civ. Code § 1798.140(l), which states that “[h]omepage’ means the introductory page of an Internet Web site *and* any Internet Web page where personal information is collected” (emphasis added).

¹⁸ Section 1798.185(a)(4) requires the Attorney General to establish rules and procedures governing opt-out requests.

¹⁹ See Cal. Civ. Code § 1798.185(a)(7) (providing that verification methods should “minimiz[e] the administrative burden on consumers”).

²⁰ See *id.* (listing other factors for the Attorney General to consider when developing regulations governing verification for responses to requests under sections 1798.110 and 1798.115).

²¹ See *id.*

²² See Cal. Civ. Code § 1798.140(y).

BSA urges the Attorney General to issue regulations that address these issues. Specifically, BSA recommends the following elements of regulations governing consumer verification and responses to verified consumer requests:

- *Flexibility in Verification Methods.* Imposing uniform or inflexible requirements for verifying consumers is unlikely to balance the objectives of verification – providing an uncomplicated way for consumers to exercise their rights and to protecting consumer privacy. Accordingly, the Attorney General’s regulations should provide businesses with sufficient flexibility to determine which technologies are best suited to their data practices and consumers’ expectations. At the same time, the Attorney General should clarify that requests made under the CCPA should come directly from consumers; and consumers may not use third parties to submit requests on their behalf, unless expressly authorized by the law.²³ A third party’s presence would make consumer verification difficult in many circumstances and would create a wide range of privacy and security risks.
- *Responsibility of Businesses to Handle Consumer Requests.* Across a wide range of circumstances, businesses have direct relationships with consumers. As a result, businesses are in the best position to receive, evaluate, and respond to consumer requests under the CCPA, and consumers should submit their requests to the relevant business. However, in at least one instance, the CCPA introduces an ambiguity into this sensible scheme. Specifically, Section 1798.105(d) lists circumstances under which a “business or a service provider shall not be required to comply with a consumer’s request to delete the consumer’s personal information . . .” (emphasis added). This language suggests that a consumer may submit deletion requests to service providers, and that service providers may be responsible for determining whether the consumer’s information is subject to any of the exceptions.

The Attorney General should clarify that Section 1798.105 in particular, and the CCPA as a whole, calls for consumers to submit requests directly to businesses and not to service providers. Such a clarification would be consistent with the overall structure and intent behind the CCPA’s consumer rights provisions.²⁴ In addition, many service providers may not have sufficient information to verify consumers who make requests. Interpreting the CCPA to allow consumers to submit requests to service providers could result in many consumer requests being denied because service providers are unable to verify the consumer.

- *Direction to Interact with Account Holders.* Although a business may not require a consumer “to create an account with the business in order to make a verifiable consumer request,”²⁵ in many instances consumers will have accounts with the business to which they wish to direct a request. For instance, a wide variety of services allow or require consumers to register or create an account for security purposes, to make payments, or to receive personalized services, among other purposes. The CCPA invites the Attorney General to consider “a password-protected account maintained by the consumer” as a factor in a business’s verification decisions,²⁶ but it does not provide further guidance on this issue.

BSA suggests that the Attorney General provide further details about the kinds of accounts that businesses may consider in verification decisions. Specifically, it would be helpful to know whether a password-protected account maintained by the consumer with the business is the only

²³ See, e.g., Cal. Civ. Code § 1798.135(a)(1) (providing that a link to opt out of sale must enable “a consumer, or a person authorized by the consumer” to make an opt-out request).

²⁴ See, e.g., Cal. Civ. Code §§1798.100(a), 105(a), 110(a), 115(a), and 120(a) (setting forth rights of consumers to make requests of businesses).

²⁵ See Cal. Civ. Code § 1798.130(a)(2).

²⁶ See Cal. Civ. Code § 1798.185(a)(7).

type that can play a role in verification. Companies that are subject to the CCPA create and maintain accounts under a wide variety of circumstances, and they would benefit from a better understanding of whether and how they may use them to verify consumer requests.

- *Procedures Following Failure of Verification.* Providing clarification on how businesses should respond when they are unable to verify a consumer would benefit businesses and consumers. In particular, regulations should relieve businesses of any obligation to consider or evaluate repeated requests from a consumer for whom verification has failed during the time period relevant to the request (e.g., the 12-month time period governing access requests²⁷).
- *Limits on Obligations Relating to Personal Information Used to Combat Fraud.* Finally, the Attorney General should issue rules that prevent verified consumer requests from becoming vehicles to undermine fraud prevention efforts.²⁸ Consumers and many companies benefit from the vibrant marketplace for services to detect and prevent fraud. Information that is considered personal under the CCPA plays a key role in developing and providing these services, and the Legislature understood the longstanding and widespread recognition of the importance of using personal information to combat fraud.²⁹ For instance, Section 1798.105(d)(2) expressly exempts from the right of deletion personal information that is used or maintained to detect or protect against fraud and a variety of other harmful activities. BSA also recognizes that a statutory amendment under consideration would allow the sale of personal information to detect fraud, security incidents, and other harmful conduct.

These statutory limits, however, are insufficient to prevent malicious actors from using the CCPA to obtain information that could compromise fraud detection and prevention efforts. In some situations, the mere fact that a business that provides fraud detection services has information about a specific consumer could reveal how its detection systems are designed or how they operate. For example, a fraud detection company's possession of a specific email address or IP address could indicate that a specific consumer has been identified as participating in potentially fraudulent activity. In addition, if the CCPA is interpreted to require highly granular disclosures about the categories of sources and recipients of personal information, malicious actors could use the CCPA to gain valuable information about the entities that provide information to the fraud detection service or that use its services.³⁰ The CCPA does not appear to provide a clear ground for the business to deny verified consumer requests for these types of information.³¹

BSA therefore recommends that the Attorney General issue regulations to clarify that businesses do not need to provide personal information to consumers or make other disclosures that are reasonably likely to compromise fraud detection and prevention efforts. The Attorney General's authority to issue such regulations includes the obligation to consider "security concerns" when developing rules governing verifiable consumer requests and discretion to adopt regulations to "further the purposes" of the CCPA.³² Data security and cybersecurity are critical to protecting consumers' privacy. Providing businesses with the flexibility to refrain from disclosing information

²⁷ See Cal. Civ. Code § 1798.130(a)(7).

²⁸ This comment uses "fraud prevention" to refer to the activities identified in Cal. Civ. Code §§ 1798.105(d)(2) and 1798.140(d)(2): detecting security incidents and protect against malicious, deceptive, fraudulent, or illegal activity.

²⁹ See, e.g., *Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 39 (2012) (identifying fraud prevention, including "practices designed to prevent security attacks or phishing," as a personal information practice that "would not typically require consumer choice").

³⁰ See Cal. Civ. Code §§ 1798.110(c), 115(c).

³¹ See Cal. Civ. Code §§ 1798.100(a), (c); 1798.110(c)(5).

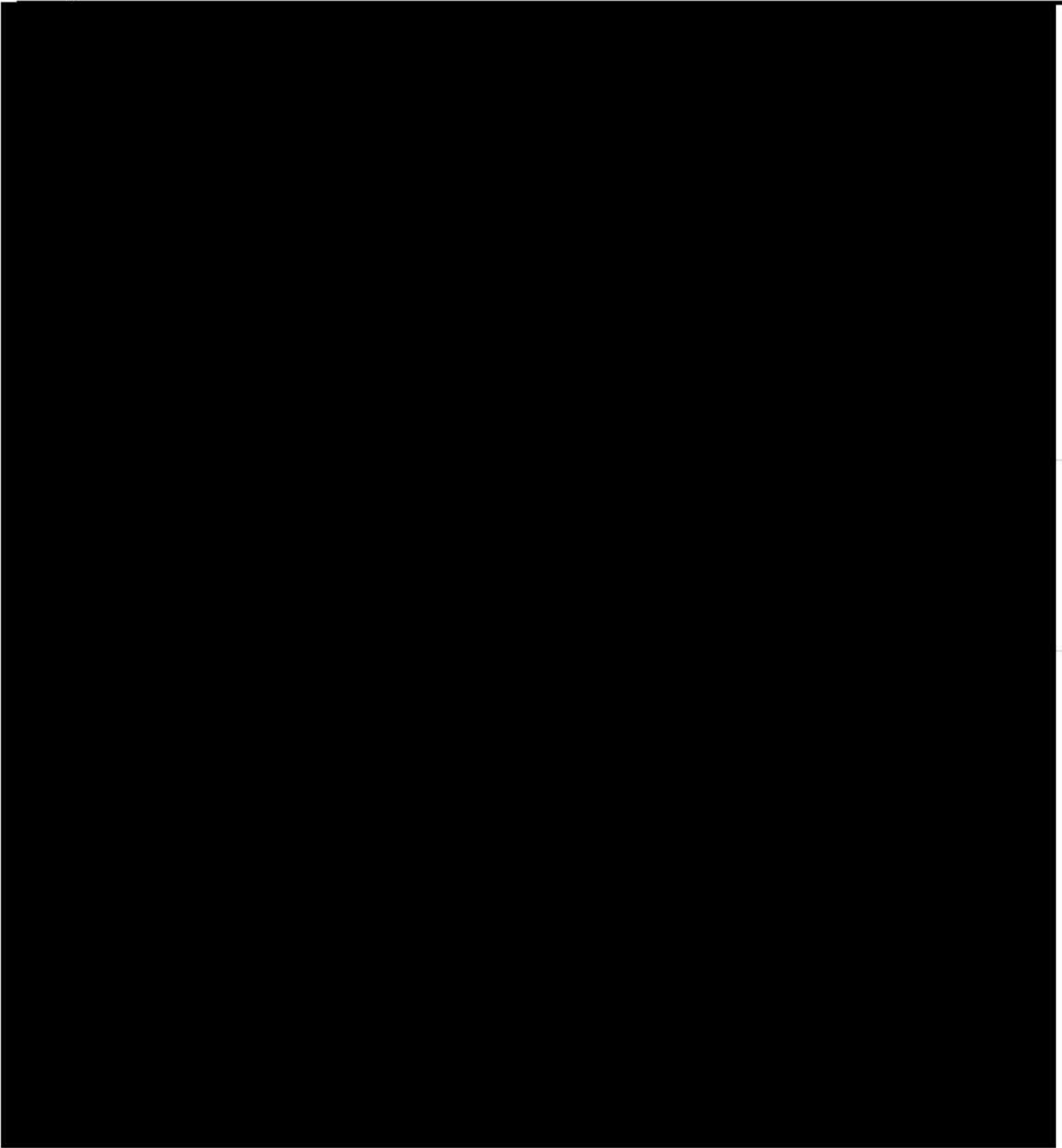
³² See Cal. Civ. Code §§ 1798.185(a)(7), (b).

that could impair fraud prevention services would be entirely consistent with this purpose of the CCPA.

* * *

BSA supports strong privacy protections for consumers and appreciates the opportunity to provide these comments. We look forward to working with the Attorney General's Office as the rulemaking process proceeds.

Message



Begin forwarded message:

From: Scott Stewart <[REDACTED]>
Date: May 20, 2019 at 10:48:28 AM PDT
To: [REDACTED]
Cc: Candace Ranglin <[REDACTED]>, Chris Grimm
[REDACTED]
Subject: Innovative Lending Platform Association and CCPA

Hi Sean,

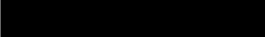
Candace Ranglin of Kabbage recently spoke with you and General Becerra at length about the CCPA and he encouraged her to submit a letter addressing our concerns through you.

The Kabbage team decided to respond to this request through the Innovative Lending Platform Association to speak to the concerns of a larger portion of the online small business lending and servicing industry.

You will find our thoughts on the CCPA implementation attached.

Thank you,
Scott

--

Scott Stewart
CEO, Innovative Lending Platform Association


May 20, 2019
Attorney General Xavier Becerra
California Department of Justice
P.O. Box 944255
Sacramento, CA 94244

Dear Attorney General Becerra,

I am writing on behalf of the Innovative Lending Platform Association (“ILPA”), a leading trade organization representing a diverse group of online lending and servicing companies that provide financial products and services to small businesses, to introduce our organization and share with you our concerns and specific requests for clarification of the California Consumer Privacy Act of 2018 (“CCPA”).

Our members exclusively serve small businesses and are committed to expanding access to capital for small businesses across the country, particularly in areas underserved by traditional financial institutions. Between 2015 and 2017, five major online lenders, including several of our member companies, funded more than \$14 billion in loans to U.S. small businesses.¹ In California, our member companies have provided over \$1 billion in capital to more than 25,000 small businesses.

Access to credit is critical for small businesses to grow. According to the annual 2019 small business credit survey conducted by 12 U.S. Federal Reserve Banks², over half (53%) of small business credit applicants experienced a financing shortfall during the prior year. ILPA members fill this critical gap by leveraging technology, data and analytics to reduce transaction costs and power lending to small businesses.

We strongly believe in protecting our customers’ data and treat the personal information of our customers carefully. We are highly supportive of the principles behind CCPA but have concerns about certain provisions that may have unintended impacts on our ability to provide much-needed capital to California small businesses. Our concerns and recommendations are set forth below:

- **Narrow Definition of “Sale”:** The definition of “sale” should be limited to the exchange of personally identifiable information for monetary considerations only, as “other valuable considerations” is too vague and could lead to conflicting conclusions by different businesses.
- **Narrow the Definition of “Consumer.”** The definition of “consumer” currently covers all California residents. Absent clarification, this can be interpreted to include both employees of covered businesses as well as individuals involved in business to business (“B2B”) transactions.
 - **Exclude Employee Information.** Employee information is governed by other laws and regulations, and coverage here could be duplicative and conflicting. Furthermore, deleting employee information collected from a person applying to or working for or on behalf of a business could impede the business from operating in its ordinary course or even, for example, result in critical evidence being expunged (i.e., in the case of an internal investigation against an employee).
 - **Exclude Individual Information Collected in B2B Transactions.** Individual information provided in connection with B2B transactions should be excluded from the definition of “consumer.” The opportunity to delete or opt out of sharing individual data in a B2B transaction could result in fraud, make diligence in B2B transactions impossible, and make it very difficult to comply with Know Your Customer and anti-money laundering laws, among others. Furthermore, the CCPA repeatedly refers to “consumer” information which, accordingly to both federal and state consumer regulations, is generally defined as

¹ NDP Analytics, The Economic Impact of Online Lending. May 2018. <http://www.ndpanalytics.com/online-lending/>

² Federal Reserve Bank, 2019 Report on Employer Firms, Small Business Credit Survey. April 2019. <https://www.fedsmallbusiness.org/medialibrary/fedsmallbusiness/files/2019/sbcs-employer-firms-report.pdf>

information obtained primarily for personal, family or household purposes and excludes information obtained for commercial or business purposes. For example, the Gramm-Leach-Bliley Act (“GLBA”), the principal federal privacy regulation applicable to financial institutions, defines consumer as “an individual who obtains...a financial product or service...that is to be used *primarily for personal, family or household purposes*.”³ Likewise, the California Financial Information Privacy Act also defines consumer as “an individual resident of this state...who obtains...from a financial institution a *financial product or service to be used primarily for personal, family, or household purposes*.”⁴ Both these definitions seek to exclude information obtained in B2B transactions, which are transactions intended to serve a commercial or business purpose. This recommendation would provide clarity for businesses complying with CCPA and achieve consistency across similar privacy regulations at the federal and state (specifically, California) levels.

- **Refine the definition of “Personal Information”:**

- **Narrow Definition of Personal Information.** The definition of “personal information” must be considerably narrowed. The current formulation covering information that “is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household” is far too broad. Theoretically, any piece of information is capable of being associated with, or can directly or indirectly be linked to, a consumer. For example, information about a business applying for a commercial loan – such as business name, business address or business email – could be deemed personal information despite the fact that the business itself is not considered a “consumer” under that definition (which covers only *natural* persons), as such business information is *capable of being associated or could be linked directly or indirectly with a particular individual*, i.e. the business owner. What is “capable of being associated with” or “reasonably be linked indirectly with a consumer” is highly subjective and broad-reaching. Businesses need clear markers and significant clarification to be able to comply with this regulation.
- **Exclude Probabilistic Identifiers.** We request that “probabilistic identifiers” be excluded from the definition of “unique personal identifier”, one of the categories of “personal information,” as these are, as their name suggests, merely predictive in nature and prone to inaccuracy. Verification based on probabilistic identifiers is difficult, and businesses may find themselves disclosing information of one consumer to another or deleting the wrong information.
- **Exclude “Anonymized,” “Deidentified,” “Aggregate,” and “Pseudonymized” Information.** Information that is “anonymized,” “deidentified” “aggregated” or “pseudonymized” should be excluded from the definition of “personal information.” Businesses frequently anonymize and aggregate information to avoid sharing sensitive information. In other words, these are privacy enhancing techniques that make the sharing of information possible without exposing sensitive consumer data.
- **Classifying “inferences drawn” as personal information:** It is currently unclear whether “personal information” includes non-public communications and content which uses or is based upon personal information, such as internally derived calculations (e.g., products and decisions generated by our member companies’ proprietary underwriting algorithms to offer capital to customers). We request that this subdivision be clarified to exclude information that is internally derived or generated and necessary for the business purpose for which the information was collected, which would make it possible for our member companies to continue providing the products and services sought by our small business customers.

- **Limit the Right of Deletion.** The right of deletion, as currently written, makes it impossible to comply with the CCPA itself and is cost prohibitive.

- **Metadata Around a Verifiable Consumer Request Must be Retained:** When honoring a verifiable consumer request for deletion, it is essential that a business retains certain metadata from the request to document that the personal information has been properly deleted and ensure that particular customer’s personal information is not re-stored in the future. If a business is not able to store such metadata, or unique identifiers or other information against which it can cross reference new data, it may inadvertently send marketing materials to a “new” customer that has previously asked to be deleted. Moreover, if a business cannot retain any information confirming

³ 12 C.F.R. § 332.3(e)(1).

⁴ Cal. Fin. Code Division 1.4, Section 4052(f).

that they executed on a request for deletion, it may be unable to defend a CCPA claim. Finally, there is certain information that must be retained for fraud detection and prevention purposes that a business may need to retain, use or share data with other parties.

- **Deleting Data from Archives and Backups is Cost Prohibitive:** It would be prohibitively difficult for a business to delete data within archives or backups, and the undue operational burden of doing so would likely increase borrowing costs for our small business customers. In order to delete data from an archive or backup, it must first be restored to a database, deleted, then pushed back into an archive or backup. In some cases, this requires complete destruction of backup media each time. Data stored in archives or backups are stored in a packaged format that is not easily readable, making it very challenging to execute the deletion request. Furthermore, actually executing on such a request has the potential to erode the quality, integrity, and credibility of the data and purpose for backup. To find the personal information of an individual consumer is analogized with destroying an entire building in order to find a single specific nail. This is extremely difficult to achieve and compromises the structure of the building itself.
- **Additional Guidance Needed on Verifying Requests.** The CCPA allows consumers to lodge a verifiable consumer request with a business whether or not they maintain an account with the business. We request clarification on how a business is expected to verify requests from consumers that are not customers or accountholders of the business. For example, many of our members purchase marketing lists containing personal information about consumers that are candidates to receive direct mail about commercial lending products. If such a consumer submits a request to a business, the business may not be able to verify the request, as the only information the business has about the consumer is often publicly available and insufficient by itself to verify the consumer's identity. Additionally, marketing databases frequently contain inaccuracies and may be unreliable for verification. Businesses cannot comply with consumer requests without clearer guidelines on the scope of verifiable requests, as they otherwise risk sharing personal information with consumers that are unverified or not properly verified.
- **Delay Implementation of CCPA Until 12 Months After Rulemaking.** The CCPA creates complex legal obligations for businesses that will require large-scale technological and operational changes, many of which are contingent on clarifications from the office of the Attorney General ("AG"). However, legislative fixes to the CCPA could continue through the end of the year, presumably after rulemaking has concluded or even started. The time and resources expended by the AG's office and covered businesses will be based on a shifting legislative and regulatory framework. Therefore, we recommend compliance with the CCPA be required no sooner than 12 months after the completion of rulemaking to allow businesses to properly and thoughtfully implement the regulations. As written, the AG's office has up to 6 months *after* the effective date to issue regulations, which means businesses may have to comply with the CCPA prior to clarification from the AG's office **and** immediately after clarifications are provided by the AG's rulemaking. This result is untenable.

We thank you for the opportunity to present our concerns with CCPA on behalf of our members and we would be happy to meet with you at your convenience to discuss these issues as you work towards clarifying guidance.

Sincerely,



Scott Stewart, CEO
Innovative Lending Platform Association

Message

[REDACTED]

From: Virginia Lam <[REDACTED]>
Sent: Thursday, May 30, 2019 8:05 AM
To: Virginia Lam <[REDACTED]>
Cc: Madelaine St. Onge <[REDACTED]>
Subject: Starry Internet files letter with FTC proposing creation of a Privacy Compact with Americans

Good morning,

Yesterday, [Starry](#), a fixed-wireless broadband provider (ISP), filed the attached letter with the Federal Trade Commission proposing the creation of a ***Privacy Compact with Americans***, to serve as guiding principles for consumer privacy protection. We believe that adopting this Privacy Compact would lay down a marker and create an easy-to-understand set of privacy commitments for consumers, who today struggle to understand their privacy rights and the government's role in protecting them.

In a world where your personal data is constantly threatened, we believe this is the right first step towards taking comprehensive action on protecting consumer privacy. We believe the FTC should act now and take a broad approach that includes internet service providers and platform providers alike.

I have attached our filing with more specific details around the Privacy Compact. Please don't hesitate to reach out with any questions.

Kind regards,
Virginia Lam Abrams
Senior Vice President Government Relations
Starry, Inc.

ABOUT STARRY, INC.

At Starry, Inc., we believe the future is wireless and that connecting people to high-quality, broadband internet should be simple and affordable. Using our innovative, next generation fixed wireless technology, Starry is deploying gigabit-capable broadband to the home without bundles, data caps, or long-term contracts. Starry is a different kind of internet service provider. We put our customers first by protecting their privacy, ensuring access to an open and neutral net, and putting the customer experience at the heart of everything we do. Headquartered in Boston and backed by world-class investors, Starry is currently available in Boston, New York, Los Angeles, Denver and Washington, DC and is expanding to 17 additional cities across the country. To learn more about Starry or to join our team, visit: starry.com.

--

Virginia Lam Abrams
SVP, Communications & Government Relations
[Starry, Inc.](#)
M: [REDACTED]
T: [REDACTED]

CCPA0001386

E: [REDACTED]



STARRY

38 Chauncy Street, 2nd Floor
Boston, MA 02111

May 29, 2019

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

***Re: Hearings on Competition and Consumer Protection in the 21st Century;
Hearing 12: the FTC's Approach to Consumer Privacy***

Chairman Simons and Commissioners:

Starry, Inc. (Starry) is encouraged that the Federal Trade Commission (FTC) is undertaking a fresh review of its approach to consumer privacy. Consumer privacy is under attack in the physical and digital realms, and the government must act quickly to upgrade and modernize its policy and enforcement frameworks to adequately protect consumer privacy. The time to act is now and the FTC is uniquely positioned to take a global leading role in privacy protection.

In order to effectively engage consumers, Starry respectfully suggests that the FTC create a ***Privacy Compact with Americans***, a set of baseline commitments on which the agency outlines its basic tenets of consumer privacy protection. This *Privacy Compact* would serve as guiding principles for the FTC and also enable the agency to iterate more detailed policies, protections, and enforcement actions over time. It is a simplistic starting point, but it's a significant improvement over the lack of any formal federal commitments.

The *Privacy Compact* would form the basis for future privacy actions without having to establish an all-encompassing framework from the ground up. Laying down a marker and creating an easy-to-understand set of privacy commitments would be a tremendous benefit to consumers, who today struggle to understand their privacy rights and the government's role in protecting them. Developing this *Privacy Compact* would be transformative to the privacy debate and create a global model.

We provide additional details and context below, and first explain how Starry, as an ISP, protects our customers' privacy.

Starry's Approach to Privacy

At Starry, our perspective on consumer privacy is simple: 1) the information we collect is the customer's information, not ours; and 2) it's our obligation to be a good steward of that information. When we collect information from our customers – or potential customers – we treat that information as theirs and use it for extremely limited purposes aimed at serving them. We strive to be as transparent as possible,

so we also consider whether a customer can easily understand - or if they would be surprised to know - how we are using a piece of information they have provided to us. If it is not clear, we continuously iterate on our policy to ensure that we adequately and clearly explain what information we are collecting and for what purpose.

We take this approach because we built a customer-centric business that does not rely on the collection, aggregation, and use of customer information, except in the most basic ways necessary to sign someone up for service and to market our service to them.

We are an ISP, and we recognize that we hold a special place in people's lives – we are the bridge to their digital life and we take that role incredibly seriously. Most importantly, we do not exploit this relationship to create other businesses or revenue streams. We generate revenue by connecting our users to the internet, and that's it. We are not a content company, a big data company, an advertising company, or a content platform. We carry this mindset through our work and our corporate culture: customer-first means providing great service, and it means protecting our customers' privacy.

Our approach to privacy can be distilled into a few key commitments, which we proudly make to all of our customers:

- When you subscribe to and use our service, we collect information for limited purposes including providing internet service, improving your internet service experience, and marketing our service and other Starry products and services to you.
- We do not sell any of the information we collect through our service, even if it is de-identified, aggregated, or otherwise obfuscated.
- We only share information about you with third parties in the limited circumstances described in our Privacy Notice, including to provide or improve our products and services, when it is required by law, or when we have your explicit consent.
- Your web browsing history is your business, not ours. We will not use or share information about the websites you visit when you are using our internet service for marketing or advertising purposes.

We also constantly strive to improve our policy and enhance transparency with our customers and will be rolling out an update to our Privacy Notice this summer to better explain how we use the data that we do collect and to meet the practices outlined in the California Consumer Privacy Act of 2018.

The Opportunity for the FTC to Make Simple, Strong Commitments

From a consumer's perspective, there is a fundamental truth about privacy – if you understand how the company that is collecting your information generates revenue, you understand what they will truly do with your data and the level of trust that you can place in them. Their actions and their need to generate shareholder value far outweigh public platitudes about privacy principles and frameworks. As the saying goes: actions speak louder than words.

In this current environment – with respect to very large platform companies, ISPs, and other large tech companies – the conventional (if somewhat cynical) wisdom is that the cost of a federal privacy regulation that is created through a process that they can influence is a far superior outcome to an antitrust process that they have much less control over. And so, these companies frequently express their willingness to cooperate on enacting strong consumer privacy protections.

We suggest that the FTC (or other agency as the Administration or Congress selects) take these companies at their word and push aggressively to enact strong consumer privacy standards and enforcement. The FTC should exert its power to the greatest extent possible and leverage this unique point in time where the current is flowing with it.

We appreciate that the FTC is taking a diligent approach to understanding the state of the art in privacy and to consider enhancing its existing case-by-case approach to privacy enforcement (to the extent it can). But time is of the essence, and the curve to a comprehensive privacy framework is steep. The FTC should act immediately to put a strong and persistent marker down now, from which it can continue shape and build a larger privacy regime.

The *Privacy Compact with Americans* is a core set of promises protecting all Americans' private information. The Compact would serve as an evergreen set of commitments on privacy that the FTC will protect through its future privacy actions. The FTC has the authority to put this *Privacy Compact* in place as a policy today. And while Congress should act to enhance the FTC's (or other agency's) authority, we believe the FTC has the authority to adopt the *Privacy Compact* as a policy statement now, without waiting for Congressional action.

We acknowledge that the *Privacy Compact* is simplistic and consumer-oriented. It is not the end game – it is a starting point from which the FTC can make a strong statement now to consumers in terms they understand, and from which the FTC (given authority) can build a more comprehensive policy framework that reflects the realities of modern technology, business models, and consumer preferences.

The Privacy Compact with Americans

We suggest that the FTC make this *Privacy Compact with Americans* with respect to their personal information:

All Personal Information is Protected Equally: All information that relates to a person's physical or digital life is personal information and should be treated the same.

Disclosure is Mandatory: Any entity that collects or uses Personal Information must explicitly and clearly explain the Personal Information it is collecting, what it will do with the information, whether they intend to sell it, and the other entities with which it intends to share the information.

Permission is Required: Personal Information can only be collected when the person agrees to have their information collected, and can only be used for the reasons that the person permits. Permission must be renewed at least annually.

Personal Information Collection Must be Minimized: Entities that collect Personal Information must collect the smallest data set necessary to achieve the purpose for which the person provided the information.

Transparency, Transferability, and Deletion are Rights: People have a right to know their Personal Information that an entity currently has, the right to receive that information in a format that is shareable and useable by another party, and the right to quickly delete that information from any entity that holds it.

Combined, these tenets provide a clear set of commitments to all Americans under which the privacy of their Personal Information is prioritized and protected. They also form the baseline from which the FTC can view and approach privacy on a going forward basis. Below we provide additional context for each clause.

All Personal Information is Protected Equally

There are not gradients of Personal Information of varying sensitivity – every single piece of information that relates to a person in a physical or digital way is personal and should be treated the same. A single piece of Personal Information is information that tells the holder something unique about a person, and any single piece of this information can be used to violate a person's privacy in digital or physical environments. And combinations of Personal Information can paint a full picture of a person's physical or digital life. Therefore, every single piece of Personal Information must be protected equally. By defining Personal Information broadly

and simply, the specific elements of information that fit within it can evolve over time.

An expansive view of what constitutes Personal Information will both train firms to collect as little Personal Information as possible and require them to protect any Personal Information in the exact same way – and in the most protective way possible.

Disclosure is Mandatory

Before any entity collects or uses any Personal Information, it must first tell the person in as specific terms as possible what information it will collect, what it will do with the information, whether or not it will sell it (individually or aggregated with other data, even if deidentified), and the third parties with which it will share the information.

A person should be able to fully and simply understand what Personal Information they are providing, why, how the collecting entity benefits, what they as an individual get out of it, and the degree to which that information will propagate away from the collecting party. Then, a person can make informed decisions about the benefit that they derive from sharing the information and whether it outweighs their perceived risk, or the value (or revenue) that that the third party derives from the information.

Permission is Required

Before any entity collects or uses any piece of Personal Information, it must first – and always – ask for the person’s permission. With full disclosure of the purpose for which the information is collected and how it will be used, the person can make an informed decision about whether or not it will permit the collector to collect or use the information. Personal information is owned by the person, not by the company collecting it, and the person should retain ultimate control over it.

People should be able to grant this permission in part – for various pieces of information and various uses. Entities collecting the information must seek the consent immediately after presenting a clear disclosure of what information it is collecting and how it will use the information. Consent must be explicit and not implied for every new collection and use, consent should be renewed at least annually.

Personal Information Collection Must be Minimized

The best way to protect people’s personal privacy is to not collect or use the information in the first place. Firms should collect the most limited set of Personal Information as necessary to provide the product or service that the person providing the information seeks. And the information that firms do collect should be directly related to the purpose for which it is collected, which in turn should be directly related to the product or service that is offered to the person. In the event that a firm collects information for a purpose other than providing the specific product or service to which the information relates – that is, it is provided in exchange for some

other good or service – this fact needs to be made clear to the person providing the information.

This is increasingly important as many firms are attempting to train Artificial Intelligence algorithms, which require huge amounts of unique pieces of data. These firms are most likely to over-collect information and use the information outside of the context of the purpose of the relationship with the user.

Transparency and Transferability are a Right

If in principle people's Personal Information is their information, then it follows that they have the right to know precisely what information any entity currently holds about them. It also follows that they have a right to take that information – their information – to another third party if they so wish.

Its infeasible for the FTC to actively police whether all firms comply with their privacy police, and too frequently failures to comply are only discovered as a result of a breach or by the actions of a whistleblower. By requiring firms to tell individuals what information the firm collected and holds, individuals become empowered to be their own check against bad actors and confirm that the collection and use is consistent with the disclosure and consent. Individuals should also be able to receive that data in a form and format that they can then share with another entity – information collection should not be a form of product or service lock-in.

Conclusion

The FTC plays a critical role in protecting consumers across a wide spectrum of areas. Consumer data privacy and protection is the new front in the war to protect consumers from criminal bad actors and deceptive corporate practices. We believe the FTC is well-positioned today to be a global leader on privacy and we look forward to working with the agency and its leadership in protecting consumers.

Respectfully Submitted,

Virginia Lam Abrams
Senior Vice President, Communications & Government Relations

Brian Regan
Vice President, Legal, Policy, and Strategy

Starry, Inc.

Message

From: Rios, Ruben [REDACTED]
Sent: 6/28/2019 12:21:24 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
CC: Avsec, Andrew J. [REDACTED]
Subject: ID Exchange Pty Ltd. re Trademark OPT OUT and Design, Reg. No. 5,299,154
Attachments: State of California Ltr re OPT OUT and Design 06-28-2019.pdf

Dear Sirs,

Please see the attached correspondence.

Sincerely,

~Ruben

Attachment

Ruben Rios on behalf of Andrew J. Avsec

Legal Secretary

[REDACTED] Direct
[REDACTED]



BRINKS GILSON & LIONE

NBC Tower - Suite 3600 | 455 N. Cityfront Plaza Drive | Chicago, IL 60611

Please Note: This message is intended for the individual or entity named above and may constitute a privileged and confidential communication. If you are not the intended recipient, please do not read, copy, use, or disclose this message. Please notify the sender by replying to this message, and then delete the message from your system. Thank you.

Andrew J. Avsec



BRINKS
GILSON
& LIONE

June 28, 2019

VIA FEDEX and privacyregulations@doj.ca.gov

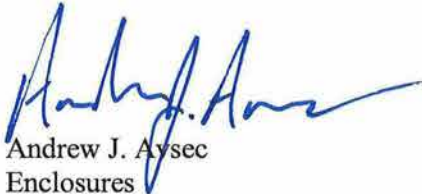
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: OPT OUT and Design Trademark (U.S. Reg. No. 5,299,154)

Dear Privacy Regulations Coordinator:

I am following up on the enclosed letter dated March 7, 2019, to which I received no response. I am writing regarding my client's OPT OUT and Design Trademark (U.S. Reg. No. 5,299,154) and the rulemaking process for the California Consumer Privacy Act (CCPA). My client would like to have a dialog about this issue at your earliest convenience. Please contact me at 

Sincerely,



Andrew J. Avsec
Enclosures

Andrew J. Avsec

March 7, 2019

BRINKS
GILSON
& LIONE

VIA FEDEX

Mr. Xavier Becerra, Esq.
State of California
Office of the Attorney General
1300 I Street
Sacramento, CA 95814-2919

Re: OPT OUT and Design Trademark (U.S. Reg. No. 5,299,154)

Dear Mr. Becerra:

We represent ID Exchange Pty Ltd (“ID Exchange”) in trademark matters.

ID Exchange was established in 2012 to develop privacy enhancing technologies (PETs) and digital rights management solutions to assist consumers to protect and mobilize their data for their benefit. Their technologies and represented platforms will provide consumers with the means to control and manage their personal data using methods such as unified instruments of consent management controls, which take the form of OPT IN and OPT OUT logos that represent different software functionality. A representative image is provided below:



A verified Opt Out® request via ID Exchange will instruct the data holder to de-identify the user’s Personally Identifiable Information (PII). This notification asks for the deletion of your name, address, email, gender, date of birth, contact number and any other PII data as stipulated under Privacy legislation.

State of California
March 7, 2019
Page 2

Often for this to be accepted by the data holder it must be compliant with data-collection "consent" regulation and the terms of the data holders Privacy Policy to which the user agreed unless the user's jurisdictional law finds the collection was not obtained in an appropriate manner.

ID Exchange is the owner of U.S. Federal Trademark Registration No. 5,299,154 for the trademark OPT OUT and Design trademark depicted below for software related to privacy management.



A copy of the federal Certificate of Registration and the full list of goods and services covered by the registration is provided at Exhibit A.

It recently came to ID Exchange's attention that the California Consumer Privacy Act of 2018 (CCPA) contains a provision requiring the development of a uniform Opt Out logo. Section 1798.185(a)(4)(C) states that the Attorney General shall solicit comments on "[t]he development and use of a recognizable and uniform opt out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information." ID Exchange is concerned that Section 1798.185(a)(4)(C) may encourage the development of a logo or button that infringes upon its trademark rights in its Opt Out mark.

ID Exchange's solution is complementary to government efforts to protect privacy. Indeed, ID Exchange is engaged with the Australian Federal government and corresponding regulator as a stakeholder and working group participant due to the forming of the new Consumer Data Right Bill (CDR) which was recently submitted to Parliament and now before the Senate, to deliver technologies aligned to emerging policy, privacy and data sharing legislation.

ID Exchange is greatly encouraged that the technology, intellectual property, and policy that ID Exchange has been developing over several years may be used to help and possibly accelerate the achievement of the CCPA's legislative objectives to the benefit of all Californians. ID Exchange is hoping to open a dialog on how its investment, knowledge and IP assets may be of benefit to assisting or collaborating with others pertaining to the rollout of such legislation.

Please contact me at your earliest convenience to discuss.

Sincerely,

Andrew J. Avsec
Enclosures

cc: California Department of Justice, ATTN: Privacy Regulations Coordinator,
(Via Email privacyregulations@doj.ca.gov)

EXHIBIT A

United States of America

United States Patent and Trademark Office



Reg. No. 5,299,154

Registered Oct. 03, 2017

Int. Cl.: 9, 42, 45

Service Mark

Trademark

Principal Register

Cloud Insurance Pty Ltd (AUSTRALIA proprietary limited company (p/l or pty. ltd.)
Level 2, 50 Bridge Street
Stone&chalk Fintech Incubator-amp Centre
Sydney, AUSTRALIA NSW2000

CLASS 9: Computer application software for computers, tablet computers, hand held computers, portable media players, and mobile devices, namely, data synchronization software, security software, password management and protection software, biometric identification, matching and authentication software, automatic notification software, data access permissions, revocations, and notifications software, database maintenance software, information storage compliance software, trust assessment software, data scrubbing and de-identification software for protection and control of users' information; Computer software for computers, tablet computers, hand held computers, portable media players, medical and mobile devices, namely, data synchronization software, security software, password management and protection software, biometric identification, matching and authentication software, automatic notification software, data access permissions, revocations, and notification software, electronic consent receipts software, database maintenance software, information storage compliance software, trust assessment software, data scrubbing software, data risk automation software for protection and control of users' information

CLASS 42: Software as a service (SAAS) services featuring software for data synchronization, security, password management and protection, biometric identification, credential matching and authentication, email account scanning, assessment of data holders to inform identity verification, authentication, and validation processes; Software as a service (SAAS) services featuring software for providing an authorized e-proxy scheme, namely, an e-proxy scheme to determine data holder access to information; Software as a service (SAAS) services featuring software for providing searching of target data holders, selection of target data holders, data access permissions, revocations and notifications, storage and maintenance of information in databases and document management systems, assuring compliance with legislation and regulations applying to personal information, data scrubbing and de-identification; Providing temporary use of a web-based software application for data synchronization, security, password management and protection, biometric identification, matching and authentication, email account scanning, assessment of data holders to inform identity verification, authentication, and validation processes, authorized e-proxy scheme to determine data holder access to information, searching of target data holders, selection of target data holders, data access permissions, revocations and notifications, storage, consent receipts and maintenance of information in databases and document management systems, assuring compliance with legislation and regulations applying to personal information, data scrubbing; Computer software design; Computer software development

CLASS 45: Identification verification services, namely, providing authentication of personal



Joseph Matol

Performing the Functions and Duties of the
Under Secretary of Commerce for
Intellectual Property and Director of the
United States Patent and Trademark Office

identification information; Digital identity access rights management for protecting data and information from unauthorized access; Personal information access rights management for protecting data and information from unauthorized access; Online privacy management, namely, authentication, assurance, validation, and revocation of digital certificates and consent receipts providing user authentication services in bilateral e-commerce transactions, open data flows, data synchronization, security, password management and protection, biometric identification, matching, and authentication

The color(s) blue and white are claimed as a feature of the mark.

PRIORITY CLAIMED UNDER SEC. 44(D) ON AUSTRALIA APPLICATION NO. 1765066, FILED 04-15-2016, REG. NO. 1765066, DATED 11-10-2016, EXPIRES 04-15-2026

The mark consists of the word "optout" and a blue circle around the letters "opt" written in white followed by the letter "out" written in blue.

SER. NO. 87-074,976, FILED 06-17-2016

REQUIREMENTS TO MAINTAIN YOUR FEDERAL TRADEMARK REGISTRATION
WARNING: YOUR REGISTRATION WILL BE CANCELLED IF YOU DO NOT FILE THE
DOCUMENTS BELOW DURING THE SPECIFIED TIME PERIODS.

Requirements in the First Ten Years*

What and When to File:

- **First Filing Deadline:** You must file a Declaration of Use (or Excusable Nonuse) between the 5th and 6th years after the registration date. See 15 U.S.C. §§1058, 1141k. If the declaration is accepted, the registration will continue in force for the remainder of the ten-year period, calculated from the registration date, unless cancelled by an order of the Commissioner for Trademarks or a federal court.
- **Second Filing Deadline:** You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between the 9th and 10th years after the registration date.* See 15 U.S.C. §1059.

Requirements in Successive Ten-Year Periods*

What and When to File:

- You must file a Declaration of Use (or Excusable Nonuse) and an Application for Renewal between every 9th and 10th-year period, calculated from the registration date.*

Grace Period Filings*

The above documents will be accepted as timely if filed within six months after the deadlines listed above with the payment of an additional fee.

***ATTENTION MADRID PROTOCOL REGISTRANTS:** The holder of an international registration with an extension of protection to the United States under the Madrid Protocol must timely file the Declarations of Use (or Excusable Nonuse) referenced above directly with the United States Patent and Trademark Office (USPTO). The time periods for filing are based on the U.S. registration date (not the international registration date). The deadlines and grace periods for the Declarations of Use (or Excusable Nonuse) are identical to those for nationally issued registrations. See 15 U.S.C. §§1058, 1141k. However, owners of international registrations do not file renewal applications at the USPTO. Instead, the holder must file a renewal of the underlying international registration at the International Bureau of the World Intellectual Property Organization, under Article 7 of the Madrid Protocol, before the expiration of each ten-year term of protection, calculated from the date of the international registration. See 15 U.S.C. §1141j. For more information and renewal forms for the international registration, see <http://www.wipo.int/madrid/en/>.

NOTE: Fees and requirements for maintaining registrations are subject to change. Please check the USPTO website for further information. With the exception of renewal applications for registered extensions of protection, you can file the registration maintenance documents referenced above online at <http://www.uspto.gov>.

NOTE: A courtesy e-mail reminder of USPTO maintenance filing deadlines will be sent to trademark owners/holders who authorize e-mail communication and maintain a current e-mail address with the USPTO. To ensure that e-mail is authorized and your address is current, please use the Trademark Electronic Application System (TEAS) Correspondence Address and Change of Owner Address Forms available at <http://www.uspto.gov>.

Message

From: Cohen, Rita [REDACTED]
Sent: 9/10/2019 12:21:03 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Letter from MPA -- The Association of Magazine Media
Attachments: Letter to CA AG Becerra 091019.docx

Please accept the attached letter from MPA – The Association of Magazine Media addressed to California Attorney General Xavier Becerra. The letter discusses the impact of the California Consumer Privacy Act for Consumers of Magazine Media.

Thank you,

Rita Cohen

Rita D. Cohen
Senior Vice President, Legislative and Regulatory Policy
MPA – The Association of Magazine Media
1211 Connecticut Avenue NW
Suite 610
Washington, DC 20036

[REDACTED] Direct
[REDACTED] Mobile

[REDACTED]
www.magazine.org

September 10, 2019

The Honorable Xavier Becerra
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Via email: privacyregulations@doj.ca.gov

Re: Impact of the California Consumer Privacy Act for Consumers of Magazine Media

Dear Attorney General Becerra:

As the primary national trade association for the consumer magazine industry, MPA - the Association of Magazine Media (“MPA”), is comprised of about 150 domestic, associate, and international members, representing over 500 magazine media brands that span a vast range of genres across print, online, mobile and video media. Our members inform, inspire and entertain more than 90 percent of all U.S. adults through the print and digital magazine titles they trust and value most. An important part of our mission is to promote a full understanding of the benefits of providing professionally researched, written, and edited content across a wide spectrum of topics.

We write to share with the California Office of the Attorney General (“OAG”) the impact the California Consumer Privacy Act (“CCPA”) could have on consumers of magazine media, the availability of magazine content, and even the viability of magazine brands. Your expedited guidance is necessary given the forthcoming effective and enforcement dates for the CCPA. Given the significant changes the CCPA will entail in data processing procedures, engineering and development teams need to finalize implementation plans and complete their work soon. For many magazine media brands, new tools will need to be developed, systems will need to be modified, and operations will need to be adjusted in order to comply with the CCPA. Absent immediate guidance from the OAG or an extension of the enforcement date, publishers may not have adequate time to properly implement the CCPA requirements in an orderly fashion, which will likely create consumer confusion in the marketplace. As detailed below, we see three particular areas of concern for magazine media:

- We want to ensure that discrimination prohibitions are interpreted in a way that allows us to continue to use different types of content revenue models, which are necessary to ensure the viability of providing content online;
- We are concerned about a lack of clarity on first parties’ liability for misuse of data when we work with third parties that may not fall into the definition of service providers; and
- We wish to avoid unnecessary risks to our readers’ privacy if businesses are forced to connect non-identifiable personal information to identifiable personal information to

satisfy access and deletion requirements in the CCPA. This can impact both our own use of data and advertising revenue models that are crucial to the continued success of magazine media.

As set forth in Section IV below, we seek guidance from your office to help us operationalize the CCPA's new standards and obligations in a way that protects consumer privacy without unduly harming our members and inhibiting consumers' ability to experience the many benefits provided by magazine media.

As an industry built on consumer trust, MPA supports the consumer protection goals of the CCPA and believes that consumers should have meaningful privacy protections, enhanced control over the use of their personal information, and greater transparency into businesses' data practices. The new law, however, has the potential to restrict consumers' access to the valuable content they enjoy and want. The CCPA, as currently written, threatens magazine publishing in a way that could drastically decrease the availability of content consumers rely upon and expect. The CCPA poses considerable challenges for MPA members and our industry as a whole. Ultimately, the perhaps unintended consequences of the CCPA will fall on our readers as the loss of magazine media voices would mean the loss of diverse information, expertise, and viewpoints that have influenced, guided, moved, and motivated people for centuries.

I. The Magazine Media Industry is Vital, Innovative and Growing.

Magazine media brands are long-standing, recognizable, and trusted by consumers. Our members communicate with authority using professionally researched, written, edited, and curated content that is delivered in safe environments, whether on digital platforms or in print. Magazine media creates powerful relationships that inform, influence, inspire, and endure. The magazine media brand experience is based on trusted editorial and reporting work, complemented and funded in part by the inclusion of relevant advertising. This dual immersion in editorial and advertising content satisfies the interests and passions of millions of readers—when, where, and how they choose, and allows access to our members' valuable content at an affordable price. The reader's commitment to this unique brand experience results in extraordinary consumer engagement with magazine media on all platforms and formats.

MPA members in particular are some of the most renowned and recognized magazine brands in the world.¹ Our members have built strong brands over decades and now engage audiences through print, web, mobile, video, social media and other platforms. Each year new magazines are launched in every part of the country. There are over 7,000 print magazine titles in the U.S., a number that has been steady for more than ten years. Last year alone, 191 new print magazine brands with a frequency of quarterly or greater were introduced, up 46% versus the prior year. As of January 2019, magazine media reached over 1.7 billion consumers globally through print, digital, web, mobile, and video platforms, up 25% in the last five years.² The

¹ MPA, *Magazine Media Companies* (2019), available at https://www.magazine.org/Magazine/Membership_Pages/Mag_Media_Members_List_2.aspx.

² MPA, *Magazine Media Factbook* (2019), available at https://www.magazine.org/Magazine/Research_and_Resources_Pages/MPA_Factbook.aspx.

magazine industry employs more than 83,000 people nationwide according to the latest data from the Bureau of Labor Statistics, including more than 8,200 in California.

II. Responsible Data Practices for the Benefit of Consumers Drives Trust in the Magazine Media Market

Magazine media brands depend on data to deliver the insightful, meaningful, and world changing content they offer to readers. Data enables magazine media brands to better understand their readers' interests and preferences in order to personalize content that is relevant to their readership. Data also plays a vital role for magazine publishers to help them reach diverse audiences that would otherwise be unaware of or not have access to their content. It allows publishers to broaden their reach and create new offerings so the industry can remain relevant to consumers and do so in a way that makes magazine media accessible and at a reasonable price. Data used by our members is generated by their readers and the broader public, and our members recognize this unique trusted relationship they have with consumers.

Consumers trust and depend on magazine publishers to deliver valuable and reliable content, news, and information to them. In fact, as of 2019, traditional media sources such as magazines outpaced online-only media, owned media, and social media in terms of consumer trust.³ Over time, consumers develop special relationships with, affinities for, and loyalties to certain magazine brands in no small part due to such brands' responsible use of consumer data and ability to provide coveted and relevant content.

In addition to data-driven content creation, magazine publishers rely on data-driven advertising to fund their content and to connect their readers with products and services that appeal to them. Advertising is a significant source of magazine revenue, reliance on which varies publisher by publisher, but, except for a small number of magazines that do not accept advertising, such revenue is crucial to magazine media's bottom line.

Studies show that consumers appreciate and favor the ad-supported model that underpins much of digital media. Eighty-five percent of consumers favor an ad-supported model, understanding that publishers responsibly use their data to personalize that advertising to be relevant to them.⁴ Our members work with advertisers and agencies to deliver the right message to readers at the right time across a multitude of channels including print, digital, mobile, and video. In the digital space, this form of advertising is often done in a privacy protective manner by not identifying specific consumers by name, email or other personally identifiable information. Instead, non-identifiable information is used to connect relevant ads to browsers and devices.

³ MPA, *Magazine Media Factbook 9* (2019), available at https://www.magazine.org/Magazine/Research_and_Resources_Pages/MPA_Factbook.aspx.

⁴ Zogby Analytics, *Public Opinion Survey on Value of the Ad-Supported Internet* (May 2016), available at http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf; PR Newswire, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth \$1,200/Year; 85% Prefer Ad-Supported Internet to Paid* (May 11, 2016), available at <http://www.prnewswire.com/news-releases/zogby-poll--americans-say-free-ad-supported-online-services-worth-1200year-85-prefer-ad-supported-internet-to-paid-300266602.html>.

Disruptions in the availability of the data that supports the magazine media industry could lead to severe negative effects for consumers, cutting off access to the most relevant news

and content that fuels readers' interests and engagement in the world at large. For example, after the passage of the European Union's General Data Protection Regulation ("GDPR") more than 1,000 U.S. based publishers blocked access to European users because those publishers were unable to adequately monetize their content under the new regulation.⁵ Additionally, following the GDPR's enforcement date the volume of programmatic advertising in Europe dropped between 25 and 40 percent across exchanges, indicating a loss of revenue for publishers.⁶ These consequences unfortunately trickled down to consumers by limiting access to information and content that enrich readers' worldview and creates a thriving democracy. Readers should be able to expect that the content that MPA members provide to them will continue without hindrance following the CCPA's implementation.

III. MPA Members Support Consumer Privacy

Magazine publishers recognize that consumers seek strong and effective data privacy protections. Our member publishers support privacy protections for consumers as such protections further bolster the consumer trust our industry has cultivated over years of responsible data use. Such consumer trust is critical to magazine media brands' relationships with their readers. MPA members believe that consumer privacy protections can be effective without inhibiting consumers' ability to connect with magazines and access content they value.

MPA has supported self-regulatory efforts to improve consumer privacy. MPA was a founding stakeholder for the primary set of self-regulatory principles that govern conduct for digital advertising. These self-regulatory tenets are known as the Digital Advertising Alliance ("DAA") Self-Regulatory Principles.⁷ The DAA is an independent non-profit that facilitates and oversees data collection, use, and transfer practices across the digital advertising ecosystem and has been hailed as "one of the great success stories in the [privacy] space."⁸ MPA supported the DAA principles and its corresponding YourAdChoices program from the beginning, demonstrating our consistent support of progressive consumer privacy tools. MPA members have long provided multiple points of access for consumers to learn about data practices and choose how they wish magazine publishers to handle their personal information.

IV. We Request the OAG's Guidance on CCPA Compliance For Three Areas of Concern

⁵ Jeff South, Nieman Lab, *More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect* (Aug 7, 2018) <http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/>.

⁶ Jessica Davies, DigiDay, *GDPR mayhem: Programmatic ad buying plummets in Europe* (May 25, 2018) <https://digiday.com/media/gdpr-mayhem-programmatic-ad-buying-plummets-europe/>.

⁷ DAA, *Self-Regulatory Principles*, located at <https://digitaladvertisingalliance.org/principles>.

⁸ Katy Bachman, *FTC's Ohlhausen Favors Privacy Self-Regulation* (June 3, 2013), available at <https://www.adweek.com/digital/ftcs-ohlhausen-favors-privacy-self-regulation-150036/>.

The CCPA sets forth a number of new requirements that impact the magazine publishing industry. As a result, flexibility in implementation mechanisms is crucial to enable magazine publishers to identify privacy protective ways to comply with the law without threatening the viability of members' business models. MPA respectfully asks the OAG to provide us with guidance regarding possible ways to operationalize the CCPA's new requirements.

In particular, we identify three key concerns for our members under the CCPA.

First, it would benefit consumers and the industry for the OAG to provide greater clarity that 'discrimination' does not include the various pricing models already in use. The CCPA's discrimination term may undermine the revenue model for magazine publishers. Specifically, this term could restrict publishers' ability to use paywalls or charge different subscription fees for access to content. Magazine brands use different revenue models to create consumer interest and maintain readership. These revenue models may include paid, free, metered use, and discount content options. Publishers require flexibility in pricing access to their content, including the use of paid subscription models, for customers that limit use of data.

Second, it is important that the OAG make clear what each party in the ecosystem's requirements are, and who liability may lay with in a given transaction. For example, the OAG could make clear which party that engages in the collection and transfer of information from a publisher's website is liable for what conduct. MPA members seek to work with reputable companies that foster privacy protective tools to engage in data-driven advertising to support magazine media. However, should one of those companies misuse data they collect from a MPA member's website or application, with no knowledge of the magazine publisher and with no reason to suspect such misuse, the OAG should make clear that the publisher in that instance is not liable for the misconduct. While the CCPA makes clear that a business is not liable for a violation of the CCPA by its service provider or when the business discloses personal information to third parties where the business does not have actual knowledge, or reason to believe, that the service provider intends to commit a violation, it is not as clear in other forms of arrangements between a publisher and other companies.⁹ Given the breadth of the definition of the term "sale," the CCPA does not make it clear which party is responsible for what conduct occurring on a website or in an application. The OAG should issue enforcement guidance instructing the industry which parties are responsible for what conduct. These type of guidance documents will provide more certainty in the marketplace, and help our members and the responsible companies they work with understand each other's roles in complying with the CCPA and in turn help consumers fully access their rights.

Third, the OAG should clarify that a business that holds non-identifiable personal information would not need to associate that data with an identified consumer or household in the context of an access or deletion request.¹⁰ While some readers consume magazine media through an authenticated account, many readers "browse" media without authenticating their identity. For readers that "browse," many magazine media brands rely on non-identifiable personal information, such as cookie IDs or other IDs that are associated with browsers or

⁹ Cal. Civ. Code § 1798.145(h), (w).

¹⁰ See Cal. Civ. Code §§ 1798.100, 105, 110, 115.

devices, to deliver content, personalize a visitor's experience, engage in analytics, and deliver relevant advertisements. These magazine media brands intentionally do not associate such information with identifiable personal information like a reader's name, email address, or phone

number. Although the CCPA states that a business need not reidentify or otherwise link non-personal information to personal information in order to fulfill a consumer request, this exemption does not cover non-identifiable data that could otherwise be considered personal information, like cookie IDs or other online identifiers.¹¹ As a result, magazine media brands may be forced to identify their non-authenticated readers, collect additional personal information about readers so they can identify them, and link their name to non-identifiable web viewing activity to respond to reader requests. This requirement creates a situation that undermines reader privacy and could negatively impact the advertising services used by magazine media brands that rely on non-identifiable personal information to subsidize access to their content. The OAG should clarify that if a business (1) implements technical and organizational measures to ensure personal information is not attributed to an identifiable natural person, and (2) makes no attempt to associate personal information with an identifiable natural person, that business is not required to reduce consumer privacy by connecting non-identifiable personal information to identifiable personal information when it processes a consumer access or deletion request. Such guidance would benefit consumers by enabling businesses to keep non-identified personal information separate from other personal information that is directly linkable to an identified consumer.

We ask that you keep magazine publishers' business model in mind as you promulgate regulations in the coming year. MPA is certain that ways exist to enhance consumer privacy by placing meaningful guardrails around businesses' sale of data while simultaneously allowing longstanding industries, like the magazine business, to remain viable and continue to provide offerings that consumers value and expect.

* * *

We thank the OAG for its consideration of this letter on behalf of our membership. MPA is committed to working with your office as it develops regulations to interpret the CCPA. If you have any questions regarding the content of this letter, please contact us at [REDACTED] or [REDACTED] or by phone at [REDACTED]

Sincerely,

Brigitte Schmidt Gwyn
Executive Vice President

Rita D Cohen
Senior Vice President

¹¹ See Cal. Civ. Code §§ 1798.140(o)(1), 145(i).

Message

From: Recht, Philip R. [REDACTED]
Sent: 10/1/2019 2:33:17 PM
To: Privacy Regulations [/o=caldoj/ou=Exchange Administrative Group
(FYDIBOHF23SPDLT)/cn=Recipients/cn=00cb2d00002f4e7c80571786b326d00d-Privacy Regulatio]
Subject: Supplemental comment letter re AG regulations
Attachments: 3731_001.pdf

Attached above please find our supplemental comments concerning CCPA rulemaking issues. These comments address recent legislative and related developments that bear on the proposed regulations. Please do not hesitate to get in touch should you have any questions.

Philip R. Recht
Mayer Brown LLP
350 S. Grand Avenue, 25th Floor
Los Angeles, CA 90071
Direct: [REDACTED]
Main: [REDACTED]
Mobile: [REDACTED]
Fax: [REDACTED]
[REDACTED]

This email and any files transmitted with it are intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

Mayer Brown is a global services provider comprising an association of legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian partnership).

Information about how we handle personal information is available in our [Privacy Notice](#).

T: [REDACTED]
F: [REDACTED]
mayerbrown.com

September 30, 2019

Philip R Recht

T: [REDACTED]
F: [REDACTED]

The California Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Re: Proposed CCPA Regulations

To whom it may concern:

Our firm represents a group of online companies that provide background report, e-commerce fraud detection, and other people search services. We send this letter to supplement our initial comment letter, dated February 13, 2019, concerning the potential content of the CCPA interpretive regulations your office is drafting.

Since our earlier comments, there have been significant legislative and related developments with respect to three of the issues addressed in the comments. Specifically, the legislature enacted AB 874, incorporating the regulatory solutions we had proposed on the topics of (1) determining what data is “capable of” constituting personal information (PI), and (2) clarifying the allowable uses of government records data. Assuming the governor signs AB 874, our proposed regulatory solutions on those issues no longer are necessary.

The legislature also enacted AB 1202, establishing a data broker registry. This development is relevant to the issue of clarifying how the pre-collection notice required under Civil Code section 1798.100(b)¹ may be provided by businesses that, like our clients, collect PI about consumers from public and other third party sources but do not have direct relationships or accounts with such consumers. As discussed below, the creation of a registry supports our suggestion that such businesses be allowed to provide pre-collection notice on their Internet homepages. It also provides an additional location—the registry itself—where businesses that are data brokers can post the notice.

Also, in recent days, the proponents of the proposed initiative that led to the enactment of the CCPA have submitted a proposed follow-up initiative called The California Consumer Privacy Act of 2020. This new initiative, intended by the proponents to strengthen the CCPA and consumer privacy rights, explicitly allows for the pre-collection notice to be provided on Internet homepages and, as such, equally supports our proposal on the topic.

¹ All further statutory references are to the Civil Code.

The California Department of Justice
September 30, 2019
Page 2

I. Nature of the pre-collection notice issue. The CCPA requires covered businesses to provide consumer notice in two instances—(1) at or before collection of a consumer’s PI (section 1798.100(b)), and (2) before sale of a consumer’s PI (section 1798.115(d)). While the CCPA specifies that a covered business must provide the pre-sale notice (i.e., an opt out link) on the business’ Internet homepage and in its online privacy policy (sections 1798.120(b), 1798.135), the CCPA does not specify how a business may or must provide the pre-collection notice.

II. Reasons why homepage notice is appropriate. There are numerous reasons why it is appropriate to allow businesses without direct consumer relationships to provide pre-collection notice on their Internet homepages. Specifically:

A. Homepage notice is the only practicable means of providing such notice. Per section 1798.100(b), the pre-collection notice, requiring a description of the categories of PI collected and the purposes for which the PI is to be used, must be provided “at or before” the PI is collected. Businesses that have direct relationships (i.e., are in direct communications) with consumers readily can (and already typically do) provide direct, individualized notice to consumers at or before collecting a consumer’s PI. For example, businesses such as Amazon, Twitter, Ebay, and Facebook that collect PI directly “from” the consumers that access the businesses’ sites all place links to their privacy policies on their homepages and require that the consumers acknowledge and approve the policies before allowing the consumers to provide their PI to the businesses.

While this is easy, indeed effortless, for businesses in direct communication with consumers, it is an impossible task for our clients and the hundreds, if not thousands, of other covered businesses that collect PI “about” consumers with whom the businesses are not in direct communication (i.e., do not have direct relationships).² This is certainly the case “before” the businesses collect the consumers’ PI since, at that time, the businesses lack any information, contact or otherwise, about the consumers. As such, direct communication with the consumers for notice or any other reason is impossible.

Notice “at” the time of collection similarly is impossible. First, much of the PI collected by these businesses (e.g., education and employment histories, social media profiles) does not contain contact information. Without contact information, individualized communication is impossible. Even when contact information is collected, it typically is unusable at the time of collection. These businesses manage literally billions of records that are obtained from thousands of sources and that arrive at the businesses in a multitude of formats. The data must

² This letter is focused on our clients’ business model of collecting public and other information about consumers with whom they do not have direct relationships. However, our clients are also e-commerce businesses that have direct relationships and communications with the consumers that use their services. This letter is not intended to suggest that our clients be excused from providing direct, individualized pre-collection notice to consumers with whom they have direct relationships. Much like the popular consumer-facing referenced on page 1 above, our clients can and will provide direct, individualized pre-collection notice to consumers with whom they have direct relationships.

The California Department of Justice
September 30, 2019
Page 3

then be sorted and manipulated into a uniform and usable format, a process that requires days, weeks, or even months to perform. The bottom line is that even when contact information is among the PI collected by these businesses, it is not usable “at” the time of collection. Thus, individualized notice is impossible then as well.³

Even when the data subsequently becomes usable, individualized notice would be impracticable and ineffectual. First, the contact information collected by these businesses from phone books, social networks, and marketing surveys—i.e., the publicly available sources typically used by these businesses—is not subject to validation requirements such as those found in the Fair Credit Reporting Act; nor does it have the accuracy of information originating from financial transactions under the Gramm-Leach-Bliley Act. As such, the contact information often is out-of-date, incomplete, or inaccurate and, as a result, cannot be counted on to result in the delivery of reliable and effective notice in numerous cases.

Second, providing direct, individualized notice to the literally tens of millions of California residents whose PI is collected in some measure by these businesses is cost-prohibitive. To send emails, texts, or postcards to this number of persons would require the businesses to engage third party services that specialize in mass communications, all at a cost of hundreds of thousands, if not millions, of dollars annually. Costs of this size would put a significant financial strain on these businesses. In some cases, it could immediately put them out of business. This would be an unjust outcome for businesses that are engaged in constitutionally-protected commercial activity involving the collection of information in the public domain and that provide services widely used and valued by law enforcement, other government agencies, businesses, and individuals and families alike.

Given all this, the best and only way that covered businesses without direct consumer relationships can provide pre-collection notice is on their Internet homepages. (As noted below, those such businesses that qualify as data brokers may additionally provide such notice on the data broker registry).⁴

B. Homepage notice is consistent with CCPA’s other notice requirement and consumer expectations. As noted, the CCPA requires that, before selling a consumer’s PI, a business provide the consumer with notice of the right to opt out of (i.e., prevent) the sale. The CCPA requires that this notice, which assumedly is equally if not more important to the

³ It has been suggested that businesses without direct consumer relationships should be allowed a period of days after the time of collection to provide individualized notice. Allowing for notice to be delayed until a later date would conflict with section 110(b)’s clear mandate for notice to be give “at or before” collection and, thus, be unlawful.

⁴ It may be possible for a business without direct consumer relationships to provide direct notice in one scenario. Specifically, to the extent a business uses technological devices such as wifi sniffers or cameras to collect PI about consumers when those consumers are at a physical location (e.g., a coffee shop), the business could provide direct (albeit not individualized) pre-collection notice to the consumers by a visible notice posted at the physical location. (We have no objection to requiring direct notice in that scenario.) However, there is no comparable scenario by which businesses that do not collect PI at physical locations could provide direct, individualized notice.

The California Department of Justice
September 30, 2019
Page 4

consumer than the pre-collection notice (which is not accompanied by any opt out right), must be provided on the business' Internet homepage. Allowing businesses without direct consumer relationships to provide pre-collection notice in the same fashion would be consistent with this approach.

It also would be consistent with the manner in which consumers typically search for online company disclosures, including those concerning company privacy policies and practices. This fact is reflected in the CCPA's broad definition of "homepage" (section 1798.140(l)), which includes an introductory page of an Internet web site, as well as a download page, a link within an app, an "about" or "information" page, or any other location that allows consumers to review the notice required by section 1798.135(a).

C. Concerns about the lack of individualized notice are mitigated by AB 1202's creation of a data broker registry. AB 1202, authored by Ass. Chau, the co-author of the CCPA, requires that businesses without direct consumer relationships that both collect and sell consumer PI—defined as "data brokers"—be listed, along with their contact information and such other information about their data collection practices as the data brokers wish to disclose, on a public registry maintained by the Attorney General. AB 1202 was intended to address the concern that, given the inability of these businesses to provide direct notice to consumers, consumers would not know of the business' existence and, thus, could not exercise their CCPA rights. As stated in committee analyses:

"Many of the CCPA's provisions require consumers to know which entities have their personal information before they can properly exercise their rights. The data brokers discussed above, by definition, do not have direct relationships with consumers and can essentially amass personal information on consumers with their permission or knowledge." (Senate Rules Committee analysis, 9/6/19, at pp. 5-6.)

"By requiring the names and contact information for these data brokers to be systematically collected and made easily accessible to consumers, the bill allows consumers to have more meaningful control over their personal information. Consumers would be able to go to this list and contact each of these data brokers to find out what information each had collected on the consumer and to demand that the data brokers cease their sales of that information if the consumer so wished." (Senate Judiciary Committee analysis, 6/21/19, at p. 7.)

AB 1202 is relevant to the pre-collection notice issue for three reasons. First, even though limited to businesses that both collect and sell PI, AB 1202 reflects the legislature's understanding, and thus confirms, that businesses without direct consumer relationships cannot feasibly provide direct, individualized notice to consumers. If direct, individualized notice was feasible by these businesses, AB 1202 and the registry it creates would be unnecessary.

Second, AB 1202 ensures that the names and contact information of these businesses will be made "easily accessible" to consumers, thus facilitating the consumers' ability to exercise their

The California Department of Justice
September 30, 2019
Page 5

various CCPA rights. In doing so, AB 1202 obviates the one and only policy concern—i.e., the potential information gap—raised with respect to allowing pre-collection notice on Internet homepages.

Third, AB 1202 permits data brokers to list on the registry any information or explanation about their data collection practices that they wish. This enables the data brokers to provide the pre-collection notice not only on their homepages but also directly on the registry itself. We would suggest that the Attorney General encourage such additional postings in its regulation.⁵

D. Requiring direct, individualized notice would be unreasonable and lead to harsh and absurd results to covered businesses and consumers alike. As noted above, and as the legislature acknowledged in its enactment of AB 1202, businesses without direct consumer relationships cannot practicably provide the pre-collection notice required under section 1798.100(b) on a direct, individualized basis. As such, requiring these businesses to do so would be unreasonable and harsh on its face.

Even if the businesses could provide such notice, requiring them to do so would result in tens of millions of California residents receiving precisely the kind of unsolicited and unwanted email, text, telephone, or mail contacts that consumers find so annoying and intrusive and that various consumer protection laws (e.g., TCPA, CAN-SPAM) are meant to prevent.⁶ Indeed, it is hard to imagine that California residents, currently beset by an onslaught of robocalls, robotexts, and spam messaging, would be pleased with yet another form of unwelcome and unnecessary communications from businesses with whom they do not have accounts or relationships, particularly in light of the creation of the data broker registry.

E. Homepage notice is consistent with the newly proposed privacy initiative, The California Consumer Privacy Act of 2020. This newly filed initiative proposal, drafted by the same persons who were the driving force behind the CCPA and intended by these persons to strengthen the CCPA and consumer privacy rights (see Sec. 2, Findings and Declarations, at E), explicitly allows for homepage notice. Specifically, the initiative would move the pre-collection notice requirement into section 1798.100(a) and then amend section 1798.100(b) to read as follows:

“A business that, acting as a third party, collects personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its Internet website. In addition, if

⁵ While we have no objections to the Attorney General requiring such posting on the registry, it would appear that such a requirement would exceed the Attorney General’s authority. As such, we suggest recommending the posting.

⁶ These businesses collect new, different, and/or updated personal information about consumers on a regular basis. Even if the businesses could provide direct, individualized notice, consumers would be annoyed, if not outraged, to receive additional notifications from the same business each time the business collects a new piece of information about the consumer.

The California Department of Justice

September 30, 2019

Page 6

the business, acting as a third party, collects personal information or authorizes another person to collect person information, about a consumer while the consumer is proximate to a physical location at which the personal information is collected, then the business shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used, and whether such personal information is sold, in a clear and conspicuous manner at such location.”

The inclusion of homepage notice in this new initiative is yet further, and highly compelling, evidence of the reasonableness and appropriateness of the concept.

III. Conclusion. For all these reasons, we reiterate our earlier request that the CCPA regulations make clear that businesses without direct consumer relationships may provide pre-collection notice on their Internet homepages.

Sincerely,



Philip R. Recht