BANK POLICY INSTITUTE

December 6, 2019

Via Electronic Mail

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

Re: Notice of Proposed Rulemaking – California Consumer Privacy Act

Dear Privacy Regulations Coordinator:

The Bank Policy Institute (BPI)[1] appreciates the opportunity to submit comments on the Attorney General's proposed regulations under the California Consumer Privacy Act.[2] BPI member banks are dedicated to protecting customer data, and they have adopted robust privacy and information security programs with administrative, technical, and physical safeguards designed to achieve that important goal. These programs are designed pursuant to and consistent with the requirements of state, federal and foreign laws, notably the federal Gramm-Leach-Bliley Act (GLBA)[3] and its implementing regulations. Therefore, BPI member banks already adhere to notice and disclosure requirements, protect the security and confidentiality of customer information, protect against anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers.[4] These programs are tailored to the size, complexity, activity, and overall risk profile of a bank, as contemplated under federal law.[5]

---

1 The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

2 Cal. Civ. Code § 1798.100 *et seq.*

3 15 U.S.C. § 6801 *et seq.*

4 As noted by President Clinton in signing the GLBA into law, the GLBA requires banks to "clearly disclose their privacy policies to customers up front…consumers will have an absolute right to know if their financial institution intends to share or sell their personal financial data, either within the corporate family or with an unaffiliated third-party [and]…will have the right to "opt out" of such information sharing with unaffiliated third parties…[and] allows privacy protection to be included in regular bank examinations…[and] grants regulators full authority to issue privacy rules and to use the full range of their enforcement powers in case of violations." William J. Clinton, Statement on Signing the Gramm-Leach-Bliley Act, November 1999. *Available at* web.archive.org/web/20160322081604/http://www.presidency.ucsb.edu/ws/?pid=56922; *accessed* Nov. 20, 2019.

5 *See, e.g.*, Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, app. B (2018).

I. Executive Summary

Given the CCPA's January 1, 2020 effective date and the separate, statutorily required, regulatory effort it is important that the Attorney General endeavor to harmonize any new requirements with the structure established by the CCPA itself. This harmonization is critical, both to allow businesses adequate time to test and implement strong compliance policies and processes and to help consumers understand their rights and responsibilities. Clarity and consistency are vital to achieving the CCPA's goal of putting consumers in control of their privacy online.

It is also crucial that the Attorney General recognize and align regulatory efforts with the long-standing and effective frameworks that banks have built over decades, under federal standards, to protect the privacy and security of consumer data. Banks already employ extensive programs in these areas, which differ from those utilized by other sectors of the economy. The regulations should take these programs into account and ensure that consumer protections are not unintentionally weakened by companies' CCPA compliance efforts.

In Part II of this letter, we propose amendments to the draft regulations to address such issues. In Part III, we describe two provisions of the regulations that, while not substantively problematic, would benefit from further clarification.

II. Proposed Amendments

A. The effective date of the regulations should be at least six months after the final regulations are published, to account for the imposition of requirements that go beyond the statute, and the Attorney General should not undertake enforcement actions for conduct that occurs before January 1, 2021.

As explained throughout these comments, the CCPA is a highly complex statute that requires businesses to invest significant time and resources in compliance. The proposed regulations, even if modified as recommended in this letter, will add additional implementation expectations to that effort, and it will take time for businesses to design, test, and implement compliant systems and processes. Many of these burdens are not contemplated by the CCPA itself, and so businesses have had less than two months to evaluate the implementation requirements of the proposed regulations, much less to invest substantial resources into compliance, given the uncertain nature of any final and binding rules. Thus, the Attorney General should provide a transitional implementation period to allow firms to establish and test compliance procedures that reflect the final regulations. Requiring businesses to compress this timeline unreasonably is likely to lead to mistakes and omissions that ultimately do not benefit consumers or the goals of the CCPA.

Section 11343.4(b)(2) of the California Government Code permits agencies to prescribe an effective date for regulations different from the default date unless the statute requires otherwise. The CCPA does not prescribe the effective date for the Attorney General's regulations, only for the CCPA itself. The Attorney General therefore has the authority to prescribe a later effective date for the regulations.

Even if the regulations are presumed to be enforceable on the same date as the statute, Section 1798.185(c) of the CCPA can reasonably be read to state that enforcement shall not begin until "six months after [1] the publication of the final regulations issued pursuant to this section or [2] July 1, 2020, whichever is sooner." That is, enforcement could be interpreted to be permitted either on January 1, 2021 or six months after the regulations are finalized, whichever is sooner. This reading is consistent with principles of fair notice and harmonizes with the legislature's clearly indicated intent to give businesses a reasonable amount of time (six months) to come into compliance with the Attorney General's regulations, which are not required to be finalized until July 1, 2020. Furthermore, it is common practice to allow such a period to give businesses a chance to interpret and implement regulations. Reading the statute to allow enforcement of the regulations on the very day they are made effective would be unjust.

The CCPA does not require the Attorney General to begin enforcement as soon as he is permitted to do so but instead leaves the commencement of enforcement efforts to the Attorney General's discretion. Thus, even if the Attorney General is statutorily empowered to begin enforcement of the final regulations on July 1, 2020, BPI would recommend that he refrain until January 1, 2021 in order to give businesses adequate time to develop compliance systems and processes, adequately test these procedures, and implement them. Doing so would better serve the interests of consumers by decreasing the risks of identity theft and security breaches that could result from hastily implemented compliance measures.

Finally, any "look back" requirements and enforcement activity should commence upon the implementation date of the CCPA regulations. Federal agencies have taken a similar approach with respect to data subject to "look back" periods in order to provide adequate time to institutions to effectively implement regulatory expectations.[6]

B. The requirement in § 999.313(d)(1) that if a business cannot verify the identity of a requestor seeking deletion it shall instead treat the request as a request to opt out of sales does not comport with the text of the CCPA or a reasonable inference of consumer intent and should be removed.

The CCPA treats the right to delete and the right to opt out of the sale of personal information as separate, placing them in distinct sections of the statute and subjecting them to distinct sets of exceptions. There does not seem to be any legal basis to convert a request to an unrequested, unrelated action because the requestor's identity could not be verified.

Additionally, without knowing who the consumer is, a business may not be able to fulfill the opt-out request or may have to opt out individuals who may not be the actual requestor, such as those who happen to share the same name. This would counter the intent of the statute to give consumers controls over their personal information, which is unreasonable and ill-advised.

If a request to delete cannot be verified, the only required action should be to inform the requestor of that fact; we therefore recommend that the attending opt-out expectations be removed. The business is separately required to provide the requisite notices and opportunities for the consumer to opt out of the sale of their information if they wish to do so.

C. Section 999.323(c)'s statement that businesses shall "generally avoid" requesting additional information from the consumer for the purpose of verification is at odds with the need to ensure verification and should be removed.

The CCPA's references to the verification of consumer requests serve as a protection of consumers' interests in the integrity and security of their personal information. It is not possible for businesses to determine with certainty at the outset what information and procedures will be necessary to verify a consumer's identity in all cases. This is particularly true because banks will be required to respond to requests from non-customers under the CCPA, and they often will not know at the outset what information they may have on such individuals that could be used for verification purposes. Discouraging businesses from asking for additional information when it is needed for reasonable verification efforts will only harm consumers and increase the likelihood of fraudulent requests. Despite efforts in the proposed regulations to decrease the value to fraudsters of submitting right-to-know requests, there is still a significant risk of disclosure of personal information to a bad actor or from the deletion of a consumer's

---

[6] For example, in 2016, the Financial Crimes Enforcement Network chose not to require identification of beneficial owners on a "look back" basis prior to the May 11, 2018 implementation date of its Customer Due Diligence rule, as it felt it would be "unduly burdensome" due to the "significant changes to processes and systems that [covered institutions were] required to implement" under the rule. *See* 81 Fed. Reg. 29,404 (May 11, 2016).

personal information against their wishes. In order to reduce these risks, the Attorney General should encourage businesses to take all reasonable steps to verify a consumer's identity before responding to a request.

BPI members and other banks have rigorous procedures in place to comply with Know Your Customer (KYC) requirements[7] that are well-suited to the verification required by the CCPA. It would better serve consumers' interests for banks to provide the full amount of protection these procedures offer, instead of watering them down for CCPA compliance purposes.

Furthermore, although the Attorney General's Statement of Reasons indicates that this provision is meant to "protect consumers by prohibiting businesses from using verification as an excuse to collect and use personal information for other means," the statute, as well as the proposed regulations, have established other safeguards to prevent such behavior. Section 1798.130(a)(7) of the CCPA requires businesses to "[u]se any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification." The second sentence of § 999.323(c) further requires that any additional information collected be used only for verification, security, or fraud-prevention purposes. Given these prohibitions, the potential harms to consumer privacy from weakened verification methods outweigh reduced risk of misuse by businesses that this regulatory language might accomplish. We therefore recommend that this language be removed from the final rule.

D. The requirement in § 999.325 that businesses provide two types of right-to-know requests with two different levels of authentication scrutiny would impose burdensome implementation requirements that go beyond the statute and do not benefit consumers.

Requiring multiple verification tiers for right to know requests, as the draft regulations contemplate, has no foundation in the statute and would not benefit consumers. Providing information even about the categories of personal information collected without adequate identity verification can pose security risks. A financial institution generally does not disclose whether a consumer has an account with it unless it is able to verify the consumer's identity. This is because bad actors can use information about the institution or other institutions with which a consumer has accounts to commit identity fraud. By providing individuals with information about data that has been collected on a consumer without verifying their identity to a high level of confidence, businesses run a significant risk of aiding identity thieves in their attempts to harm consumers.

If a business chooses to have multiple tiers of verification based on the sensitivity of the data and the level of risk, that should be permitted, but it should not be a requirement placed on all entities. The Initial Statement of Reasons does not specify why this differentiation is "reasonably necessary" to protect consumer privacy, nor does it address the concern that such an approach could actually result in identity theft. The regulations should instead encourage businesses to take all reasonably necessary steps—including use of existing KYC procedures, if they exist—to verify a consumer's identity before responding to a request. This aligns with the guidelines established by § 999.323(b)(3) of the draft regulations.

Relatedly, BPI requests that the Attorney General clarify that the requirement in §§ 999.308(b)(1)(c)-(b)(2)(c) and § 999.313(a) that a business describe the process used to verify consumer requests, including any information the consumer must provide, may be satisfied with a description at a high level of generality. Requiring more detailed descriptions of verification processes could aid bad actors in their efforts to exploit the system for fraudulent purposes. This is particularly true for banks, where information gathered about an individual's accounts with one institution is often used by identity thieves to attempt to gain access to accounts or to create new accounts at other institutions.

---

[7] Although the term "KYC" is not used in regulations, it is generally used in industry and regulator parlance to refer to institutions' obligations to collect, analyze, and use information about their customers to comply with various anti-money laundering and sanctions requirements that require financial institutions to understand, to some extent, the nature and identities of the parties with whom or on whose behalf they are conducting financial transactions.

E. Requiring publication of metrics regarding responses to consumer requests in a business's privacy policy, as § 999.317(g) would, will not benefit consumers, but could increase the risk of identity fraud. These metrics should instead be provided upon request to the AG.

The metrics described by § 999.317(g) are intended to gauge a company's compliance with the CCPA. Since the statute is enforced by the Attorney General and not by the consumers for whom a privacy policy is drafted, it would be more appropriate for businesses to be required to provide them to the Attorney General upon request. Placing them in the privacy policy would only serve to increase the length and complexity of a document that is intended to be digestible by consumers, without providing them any useful information about how their personal information is collected or used. In addition, the posting of metrics provides additional information for fraudsters looking to attack companies with fraudulent requests. For example, businesses with metrics showing a high rate of fulfilling requests are likely to become victims of fraudulent requests, where fraudsters may avoid a business with metrics showing a high percentage of access request denials. Finally, such an approach is in line with Section 11346.3(a) of the California Administrative Procedure Act, which states that an agency must consider the impact on California businesses and avoid imposing "unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements."

F. The requirement in § 999.313(d)(4) that a business must specify the manner in which it has deleted information is burdensome, confusing, and unnecessary, and it should be removed.

In a large business, the process of responding to a request to delete personal information will be complicated, likely involving many systems and business units. Some data elements may be deleted outright, while others are deidentified, or otherwise modified to place them outside the scope of the CCPA's definition of personal information. Providing a detailed description of this process would be burdensome and, rather than providing "greater transparency about the business's practices in deleting personal information" as the Initial Statement of Reasons contemplates, would in fact create confusion for consumers. For example, consumers may not appreciate the differences between deletion, deidentification, and aggregation. Businesses should instead be permitted to simply inform a consumer that their personal information has been deleted, or to inform them of the reasons it has not been deleted, as provided by § 999.313(d)(6) of the proposed regulations.

G. Section 999.305(d)'s requirement that a business obtain attestations of compliance from third-party collectors if the business does not directly collect information from a consumer is confusing and lacks statutory basis.

Under § 999.305(d), a business is not required to provide initial notice if it is not directly collecting personal information from the consumer. However, this provision requires that businesses ensure that the party that provided (sourced) the data gave the consumer the initial notice mandated by the CCPA. It also requires that businesses retain a "signed attestation" by that party to confirm the third party's adherence with the initial-notice requirement.

This requirement is problematic because it places the burden on the business receiving data to confirm that all parties who are sourcing data are complying with their CCPA notice obligations. The requirement has no basis in the text of the CCPA. Third parties who provide data should be the ones maintaining any documentation of their compliance with their notice obligations, in line with the provisions set forth in Civil Code section 1798.115(d).

H. The requirement in §§ 999.305(b)(2), 999.308(b)(1)d.2, and 999.313(c)(10) that information be presented category by category rather than in the aggregate—contrary to how the language of the CCPA is reasonably read—will result in consumer confusion and should be removed.

Given the level of detail that the proposed regulations would require in these sections, consumers are likely to be overwhelmed by the quantity of information, without providing a more meaningful understanding of a business's

data practices. There are 11 CCPA categories of personal information, a proposed minimum of three source types, and seven third-party types, along with an uncertain number of uses or purposes of collection, all of which businesses would be required to describe both in a privacy notice and in customized responses to access requests. Under the draft regulations' approach of requiring this information to be described "category by category," which goes beyond a reasonable interpretation of the statute's requirements, this could require many additional pages to communicate the various permutations of these pieces of information. Even for a business of moderate complexity, for example, a notice could run to more than 20 pages. This would be overwhelming to consumers, and it is unclear if and how this information could be presented on a small screen, as the draft regulations require.

These provisions would impose a large administrative burden on businesses of all sizes, without meaningfully adding to consumers' understanding—and, in fact, quite possibly detracting from it. Therefore, we recommend that it be limited, as it is under the statute, to personal information that is sold.

I. Section 999.306(d)(2) appears to require that a business that begins selling personal information obtains opt-in consent from every consumer who the business has previously interacted with. This would be extremely burdensome and lacks statutory basis.

If a business that has not previously sold personal information decides to begin doing so—or if an aggressive interpretation of the CCPA's definition of "sale" is adopted that encompasses practices a business did not believe were included—§ 999.306(d)(1) prohibits it from selling information collected during the period when it did not post a notice of right to opt-out. This limitation is sufficient to provide the protection for consumers intended by the CCPA's right to opt out from sale. Consumers who interact with a business that does not sell their information have not thereby expressed any affirmative desire to opt out of the sale of their information, and it would be in tension with the statutory framework to treat them differently from other consumers.

Additionally, it may be very difficult or impossible for a business to implement this provision. Determining all consumers whose personal information may have been previously collected and contacting them to obtain consent may not be possible, depending on the information a business maintains. Instead, businesses should be prohibited from selling information that was collected without the proper notices in place, and they should be required to adhere to the practices disclosed at the time of collection for that data going forward (unless opt-in consent is obtained), but they should not be restricted from changing their practices and providing the same CCPA rights as any other business in relation to data collected in the future. BPI would recommend that businesses be required to give consumers a reasonable period of time to opt out after the requisite notices are provided, as is required, for example, by the GLBA.[8]

J. The 12-month lookback in the regulations and the statute should not be enforced in relation to conduct occurring before the effective date of the CCPA.

As of January 1, 2020, when the CCPA is effective, businesses will be required to make various disclosures about their practices for the past 12 months regarding collection, use, and sale of personal information. However, since the CCPA's definitions, particularly those of "sale" and "personal information" differ significantly from definitions in other statutes, some businesses may have difficulty ascertaining the precise set of data points they collected or transfers they engaged in that would fit these definitions. Accordingly, BPI would recommend that the Attorney General not bring enforcement actions based on disclosures of conduct occurring before the effective date of the CCPA, as long as businesses make reasonable efforts to give consumers an understanding of their practices.

---

[8] *See* 16 CFR § 680.24.

K. Section 999.325(e)(2)'s instruction that businesses use a "fact-based verification process" for information not associated with a particular consumer should be removed.

For personal information that is not associated with a "named actual person," businesses are advised in § 999.325(e)(2) to conduct a "fact-based verification process" to allow a consumer to show that they are the only person associated with the personal information. This provision appears to require businesses to reidentify or link information that is not maintained in a manner that would be considered personal information, in contradiction of the CCPA.[9] BPI requests that this provision be removed, or that the Attorney General clarify that the provision is a recommendation rather than a requirement and that it does not require re-linking of non-personal information. Additionally, if the provision is retained, BPI requests that the Attorney General clarify the meaning of the term "fact-based verification process."

III. Requests for Clarification

A. The regulations should clarify that consumers should not be able to skirt the rules of discovery during litigation by exercising rights under the CCPA.

The regulations should consider—and affirmatively prevent—the ability of a consumer to initiate a CCPA access or deletion request in lieu of discovery in a court matter. If not prevented, individuals would be able to circumvent established legal discovery rules under the false pretense of exercising a state-law privacy right. BPI requests that the Attorney General clarify that Section 1798.145(a)(4) of the CCPA, which states that the law shall not restrict a business's ability to "[e]xercise or defend legal claims" prevents this sort of avoidance of discovery rules.

B. The regulations should clarify that § 999.306(d)(2) does not restrict a business from changing its practices to begin selling personal information, if proper notice is given and opt-out mechanisms are provided.

Section 999.306(d)(2) requires that, for a business to be exempt from providing a notice of right to opt-out, it must "state in its privacy policy that it does not **and will not** sell personal information" (emphasis added). On its face, this would appear to restrict a business that does not sell information (and that therefore does not provide a notice of right to opt-out) from ever changing this practice. However, § 999.306(d)(1) plainly contemplates that the business only must refrain from selling information collected during the time period during which the notice of right to opt-out is not provided. BPI requests that the Attorney General clarify that § 999.306(d)(2) merely requires a business to state that it will not sell personal information collected during the time period during which the notice of right to opt-out is not provided.

*****

The Bank Policy Institute appreciates the opportunity to submit comments concerning the Attorney General's draft regulations. If you have any questions, please contact the undersigned by phone at 202-589-1935 or by email at *Angelena.Bradfield@bpi.com*.

Respectfully submitted,

Angelena Bradfield

Angelena Bradfield
Senior Vice President, AML/BSA, Sanctions & Privacy
Bank Policy Institute

---

9 *See* Cal. Civ. Code § 1798.100(e).