MEDIA ALLIANCE

December 27, 2018

California Department of Justice
Attn: Privacy Regulations Coordinator
300 South Spring Street
Los Angeles CA 90013

**Re: Implementation of California Consumer Privacy Act of 2018**

The regulatory framework for the 2020 implementation of the California Consumer Privacy Act of 2018 is a significant task for the CAL-DOJ. Since no other state has passed as ambitous and comprehensive a consumer privacy framework as California's CCPA, the DOJ must flesh out an innovative and expansive protocol to implement this law, while grappling with some inconsistencies in the existing text related to the speedy approval process in the CA Legislature and a raft of competing interests. We do not envy your task.

Our comments today are narrowly focused on the pay for privacy implications [1] of the law's current text and the implementation choices that the CAL-DOJ must make. We will discuss some potential problems and concerns and then provide some recommendations for what we believe to be the best possible protocol within the constraints of the current legislative language. Nothing stated here is intended to forestall modifications/improvements to the existing language via the Sacramento legislative process in 2019. To whatever extent the DOJ finds the issues raised here compelling, we would hope for your institutional support for some consumer-protective additions.

Media Alliance is working in partnership with numerous other privacy advocates on the implementation of CCPA. We believe our comments here are consistent with the views of many other privacy groups at least in the broad scope of our concerns, but these recommendations are solely those of our particular organization and should not be taken as a summary of the views of any other privacy advocacy organization.

Media Alliance is a Bay Area democratic communications advocate. Our members include professional and citizen journalists and community-based media and communications professionals who work with the media and on various digital platforms powered by the Internet. As an organization, we particularly focus our advocacy on communications by and for marginalized communities and alternative points of view, with an understanding of how resource inequities affect the nature of the public dialogue on an ongoing basis and the challenges faced by consumers of limited or inadequate means.



1 https://www.akingump.com/en/news-insights/california-passes-landmark-consumer-privacy-act-what-it-means.html

While the much-publicized "privacy problems" of the past few years including Cambridge Analytica [2] and Equifax [3], have had broad impacts on all consumers, there is no doubt consumers of limited means often get the double whammy of the most impact and the least ability to mitigate those impacts through services like credit monitoring, attorneys and the court system, and online assistance in the form of software fixes and jargon-filled guides. [4] Among others, SUNY-Albany professor Virginia Eubanks has written extensively on how privacy abuses manifest in very different ways for lower-income and higher-income people in *Automating Inequality* and *Digital Dead End*.

One of our critiques of CCPA in its current form is that given the origin of much of the language in a ballot initiative developed by a wealthy real estate developer, the finished language of the bill is not always as attuned as it could be to the specific privacy challenges faced by lower-income communities. It is understandable that such issues may not have been front and center in the ballot initiative's drafting. But at this juncture, it is your task, and one that we hope you embrace, to craft a regulatory structure that makes the law operational and functional for all Californians, including those of limited financial means.

Using this lens, we turn to the existing pay for privacy language in the current text of CCPA, namely section 1798.125, reproduced below for convenient access. We also cite section 1798.185 Sections 4(A) and 4(B) and 7 to indicate that the recommendations contained herein are firmly within the DOJ mandate.

**1798.125.** [5]

*(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:*
*(A) Denying goods or services to the consumer.*
*(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.*
*(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.*
*(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.*
*(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.*



2 https://www.theguardian.com/uk-news/2018/dec/23/cambridge-analytica-facebook-scoop-carole-cadwalladr-shocked-world-truth-still-elusive
3 https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496
4 https://motherboard.vice.com/en_us/article/ypwe9x/why-mass-surveillance-is-worse-for-poor-people
5 https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375

*(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.*
*(2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.*
*(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.*
*(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.*

In turning to this language, we want to address practical imports. The text in the California Consumer Privacy Act is clear in the intention to prevent consumers from being discriminated against for choosing to opt out of sales of their data, including facing pricing differentials that are in any way coercive, unreasonable or unjust. We believe this language reflects the intent of the Legislature, [6] which recognizes that it is problematic to establish a right, and then allow that right to become overly burdensome or difficult to execute.

Out of a seeming concern for business models which rely on the sale of customer data for a significant amount of their income stream, the language then provides a pay for privacy clause. The clause permits consumers who choose to opt out to be given a different price or rate or to be denied a discount because of their choice to opt out, as long as the discrimination is reasonably related to the value of their data.

As has been discussed, CCPA's current language states the criteria as "reasonably related to the value provided to the consumer by the consumer's data". This is a confusing phrase, at best, since consumers will have different interpretations of the value of their data. Additionally, that value will differ depending on the nature of the data collected (i.e. my email address and the fact that I like suede boots is probably of less value to me than facts about my medical status, my home address or the state of my finances). Even using the interpretation that the phrase refers to the value of the customer's data **to the business** (i.e. how much it can be sold for to other parties), the phrase leads to an inconsistent standard as the market value for data is likely connected to the nature of the specific data collected. This leaves "reasonableness" with a not clearly quantifiable number across different business models and transactions. Privacy conscious consumers would not be entirely cognizant of the potential expenses of utiizing the opt out, even if companies follow the regulations scrupulously.
We are not entirely convinced that the average consumer has an intricate enough knowledge of the ins and outs of the data sale marketplace to assess if a business is correctly quoting the value of their data [7] or going for as much as they think they can get without a complaint being filed for unreasonableness.



6 https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375
7 https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa

Also relevant is the simple reality that California has the highest cost of living in the United States. Many Californians are financially struggling with preposterously high rents and/or mortgages and crushing student loan debt.[8] Workers trapped in lower-wage jobs in retail and service industries suffer from housing instability and those on fixed incomes can barely pay their bills. Even working adults with well-paying jobs are often living paycheck to paycheck.

This does not, in any way, mean that financially struggling Californians are not concerned about what companies are doing with their data. Every poll shows that a large majority are very concerned about the uses of their data and feel a lack of control about where it ends up.[9] But the impact it has in a practical sense, is to apply a cap to the number of times that many California residents are going to be able or willing to reimburse a company for the value of their data in order to avoid having it sold on the open market.

There is no doubt that consumers will vary greatly in the amount and nature of data-driven transactions they participate in and that would be subject to CCPA. Some engage in frequent online transactions, some do not. Some make efforts to use small local businesses as much as possible, others are frequent customers of huge national and international companies.

But one thing is certain. The vast majority of consumers engage in numerous transactions every year that are likely subject to CCPA: their ISP, their wireless provider, various social media platforms, and several service providers and retail outlets every year. The opt-out and pay the company for your privacy choice will be in front of California consumers over and over again.

A modest fee of $5/year for your data, or $10/year, or $20/year, all fees that most people might consider in the reasonable range become increasingly less reasonable when replicated 10 times a year or 20 times a year or 30 times a year.

While it is true consumers do not have to adopt a global opt-out or opt-in position, it is also true that assessing the best use of an annual $50 or $100 privacy budget among the multiplicity of companies who collect your data is a task more suited to a privacy expert than a busy single mom. Do you pick your ISP? Or Facebook? What about Amazon? The national pharmacy chain where you fill your prescriptions? [10] And on and on.

While surely a cottage industry will develop in advising people how best to opt out, it is perhaps naive to expect that advice will reach everyone, or even most of the people who might need or want it.

For the most economically vulnerable communities, no advice in the world will make an extra $50 present when it isn't there. We have been privacy advocates long enough to know that in a contest between privacy protection and food on the table, food on the table will win every single time.



8 https://www.kqed.org/news/11689103/survey-nearly-half-of-working-californians-struggling-to-make-ends-meet
9 https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds
10 https://medium.com/bestcompany/5-companies-that-have-been-caught-violating-their-customers-privacy-9cfe660ea3eb

The financial incentive language in CCPA probably has its origin in beliefs by businesses that rely on the sale of personal data that if customers are notified their data is being sold, large numbers of them will choose to opt out. By its nature, this is a speculation. [11]

Given that we are dealing with a brand new law and consumers have never before received comprehensive information about how extensively their data is being sold, it is a guessing game to estimate how many will shrug, and how many will fill out the opt-out form. But if those with the most direct knowledge of data sale practices are convinced transparency will lead to a scale of opt-outs that will threaten their business models, then they are probably in the best position to make that guess.

So we will take it at face value that the problem here is two-fold.

- Firstly, that consumers may be pecked to death with small opt-out fees to such an extent that their ability and willingness to make free decisions about their privacy will be compromised by financial worries;

- Secondly, that many businesses may face such extensive opt-outs that their business model will be challenged, if not totally rendered unworkable;

As the AG's office navigates these interests, we want to note that there are distinctions to be made about the nature of affected transactional relationships and the affected business models.

In the first example, the nature of the transactions are the customer purchasing an item or service for a set price. While doing so, they provide data including their contact information, their product preferences and interests, and other related data. A business may then engage in collateral monetization of that collected data, usually without much knowledge by the customer who paid little-to-no attention to the lengthy privacy policy disclosing their info may be shared with third party partners.

In a simple example, I buy a hat on-line from a hat company. The hat company may have a collateral activity of selling their customer data to a company which then provides lists to sellers of similiarly styled apparel items. In a broader sense, consumers pay their Internet Service Provider (ISP) for the ability to connect to the Internet. In this case, the fundamental transaction is not for the customer's data per se, but for a product or service - with the generated browsing data and any actual or potential monetizationof it as a collateral activity. We will call these companies product providers.

The second example is companies that provide a service or product for free and engage in third party monetization of collected customer data as their fundamental source of income. This is a popular model for technology companies, including much of the social media Californians rely on.



11 https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules

To go back to our hat example, a tech company might offer online a free hat reference service that directs potential customers to possible sources for different kinds of hats with comparative pricing and availability info. All for free, as long as they enter some data about their location, contact information, and consumer preferences into a form. Consumers often choose to use such services because they are convenient and save time. The company then has a data trove of interest to apparel companies everywhere and can and does monetize that collected data to support the costs of operating the referral site.

In this model, consumers generally suspect that their data is the product, expect they may see a few ads in the mail or on their screens in the future, and are sacrificing privacy about their consumer preferences in exchange for some convenience.

But it is fair to say that in at least some cases, users (as these individuals are not customers in the traditional sense of the word) may not be aware of the range of monetization activities and they may exceed the scope of their expectations. [12] So companies using this business model have some expectation that transparent disclosure of how user data is monetized will may lead to a significant number of opt-outs. Like any business, they are justificably terrified that the law will essentially break their business model and deprive them of their fundamental income stream. We will call these companies data providers.

It is our belief that a pay for privacy regulatory protocol would benefit greatly from separating these two categories of businesses to the extent legally permissable in the existing language. This would allow the law to address their needs independently, as they are not fundamentally the same.

Consumers are paying product provider companies for the service or product they are receiving. They reasonably think the price they pay is for the purpose of covering the company's costs for goods and labor to provide the product or service, and the data they provide to the company is primarily for the purpose of filling their order. In the free market economic model, a company adjusts the price for their product or service if what they are charging does not cover their costs and allow for some level of profit.

For product provider companies, we believe it is largely inappropriate for consumers to be charged twice, once for the product or service they bought, and once to halt the sale of the data they were required to submit in order to obtain the product.

We would recommend that product provider companies, since they have the discretion to adjust product prices to account for any loss of income from customer opt-outs, be prohibited from giving customers less advantageous prices for choosing to opt-out.

In the language of CCPA, the value of a customer's data to a business whose primary business is not data, can be mathematically defined as $0. In practical terms the value of the data can be recompensed through product pricing. The fundamental business model here is product-based transactions, not the sale of data to third parties.



12 https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1177&context=qc_pubs

This would protect consumers from a veritable flood of privacy-based fees by imposing enough market discipline that companies would raise prices only in the face of documented losses of revenue from CCPA opt-outs. Rather than what might otherwise happen with companies trying to de-incentivize opt-outs in advance with punitive pricing by default that is targeted only at privacy-protective customers.

For data providers, companies that provide free services in exchange for customer data that are then monetized as the primary function, it is understandable that CCPA provides a potentially existential crisis. If a substantial chunk or even most of the users opt out of data sales, the companies stand to go out of business.

We believe that it is these companies who the pay for privacy clause in CCPA is largely meant to protect. And deservedly so, at least to the extent they are offering services and products people want to use and for which users are willing to surrender their data in order to get them free of charge.

The problem for such companies in a post-CCPA world is that the exact nature of the deal may not have been clear to their users. Users understand that nothing is free (as in the old joke, if you don't know what the product is, rest assured that it is you), but they may not have been aware of the full extent of how their data was monetized. The risk that CCPA carries for such companies is that the transparency requirements will convince their users that the deal is a bad deal and they will lose them in such quantity that they can no longer cover their operating costs.

For such companies, a price different than free for a formerly free service may be the only way they can survive with a user base that partially or even substantially chooses to opt out of data sales. We agree that it may be necessary for such companies to reserve the free pricing of the service for users that permit the monetization of their data.

However, such a change should be as reality-based as possible. We'd like to see such pricing changes linked to verifiable data that users of a formerly free service have chosen to opt out of data sales in sufficient numbers. Pricing changes, especially in widely used services, should be necessary, not gratuitous or speculative.

We'd also like to have the numbers that are assessed as “the value of the customer's data” vetted for reasonableness, justness, non-coerciveness and non-usioriousness by the AG's office in advance of users being charged.

We envision a possible roll out of transparency requirements and opt-out notifications preceding any pay-for-privacy charges being levied. Armed with data about the what initial opt-out levels actually are, the AG would receive proposed non-advantageous pricing for opt-outs in 2021 and approve they are compatible with the law and meet standards for being reasonably related to the value of the data and are just, reasonable, non-coercive and not usurious.

We consider this to have two significant advantages:

- Firstly that the AG's office will not be overrun with complaints that pricing changes are neither just nor reasonable

- Secondly that better business decisions will be made with data on hand rather than speculation about how many users may choose to opt out.

We would hate to see users, especially low-income users, crowded off, for example, social networks that are important to many for connecting to friends and family and participating in civic dialogue, by sky-is-falling projections by data provider companies that are fear-based instead of fact-based.

One of the most contentious areas in the pay-for-privacy arena has been so-called “customer loyalty” programs which give users preferential pricing. Some businesses in the product provider category have indicated CCPA's language would prohibit such programs, which are popular with customers.

We are not sure that it is the case, for two reasons.

- Firstly, there is the intent of such programs. As we understand them, they are reward programs, but the reward is not for the provision of the customer's personal data to the company, but for the customer's loyalty i.e. their repeated purchases of the company's product or services. Accordingly the preferential pricing or discounts and/or gifts to the customer are not, by definition, reasonably related to the value of the customer's data. The incentivization is not to decline to opt out of data sales, but to repeatedly patronize the business.

- Secondly, there is the mode of selection. CCPA protocol allows an opt out of data sales. If customers do not affirmatively take action to opt out of data sales, then by definition, they have passively opted in. However CCPA's language adds a second bar for loyalty programs. The customer must affirmatively opt in.

The constraints applied by CCPA regarding pricing incentives is specific. The wording is relative to exercising the consumer's rights under the title.

With regard to financial incentive programs like loyalty programs, CCPA refers to section 1798.35.

*A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.*
*A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time*.

Section 1798.135 specifies the requirement to provide a clear and conspicuous form to allow customers to opt out. The language in CCPA referring to discrimination with regard to financial incentives is specific to customers who exercise their right to **opt out**. Not those who exercise their right to voluntarily and affirmatively opt in to loyalty or discount programs.

There are three sets of customers:

- Those who **choose to opt-out**;
- Those who a**ffirmatively and voluntarily opt-in** to preferential pricing/discount/loyalty programs;
- Those who **do neither.**

CCPA's price discrimination language is directed at groups (1) and (3), specifically protecting group (1), who are exercising their rights under this title from being discriminated against relative to group (3), who are not choosing to exercise their rights under this title. Group (2) is affirmatively choosing to sell their data on a voluntary basis in order to get better pricing or goodies. Treating them identically to customers who passively fail to exercise their right to opt out would seem like a misreading of the text.

In other words, we would consider the language in CCPA to be intended to waive customers who intentionally opt in to loyalty programs from the language cited below, as the customer is affirmatively choosing not to exercise their right to opt-out under the title.

*Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.*
*Providing a different level or quality of goods or services to the consumer,* ***if the consumer exercises the consumer's rights under this title.***

Media Alliance believes the language in this section was intended to exempt product provider company's loyalty discount programs from the preferential pricing prohibition, and was simply poorly written.

This distinction between opting out affirmatively, passively failing to opt out, and opting in affirmatively is significant in both understanding and functionally implementing the law as written. We hope it is one the Attorney General will recognize as such. The distinction will greatly assist efforts to protect consumers from untoward financial burdens should they wish to protect their private data from sales to third parties.

We believe the conflation of a passive failure to opt out and an affirmative choice to opt in to a loyalty program, whether accidental in the drafting or not, will be a strong contributor to industry frustration with the law and it's purported "unworkability". Untangling that conflation in the regulatory process would be a meaningful step in the real world implementation of CCPA.

We will add that the privacy community's general support for a global opt-in protocol, rather than an opt-out option, are at least partially based on the increased clarity provided by the global opt-in. But the regulatory process can only address the language in hand. The language in hand provides, we believe, sufficient grounds to exempt loyalty programs customers affirmatively choose from CCPA's differential pricing prohibition.

This clarification focuses the discrimination provisions where they belong; the two choices made by users and customers pursuant to the law: the decision to opt out of data sales or not to utilize the opt-out option.

**Summary of Recommendations:**

1) **Separate CCPA-impacted companies according to whether or not they charge for their products or services.**
2) **Set the value of a consumer's data to a business that charges for their product or service to their customers or users to $0.**
3) **For businesses that provide free products or services, vet proposals for less advantageous pricing for users that opt out on receipt of opt-out statistics and demonstration of reasonableness.**
4) **Exempt customer loyalty programs from the differential pricing constraints in CCPA since customers affirmatively opt-in to such programs and by doing so are not exercising their rights under this title.**

Thank you for the opportunity to provide these comments.

We look forward to the 2020 implementation of the California Consumer Privacy Act of 2018.

We are proud of California for leading the way in consumer privacy protections.

Respectfully,

Tracy Rosenberg

Tracy Rosenberg
Executive Director
Media Alliance
2830 20th Street, Suite 102
San Francisco CA 94110
Email: tracy@media-alliance.org
Web: htttps://media-alliance.org