



March 8, 2019

Attorney General Xavier Becerra
P.O. Box 944255
Sacramento, CA 94244-2550

Via email: privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act – Rulemaking Process

Dear Attorney General Becerra:

Consumer Watchdog thanks you for the opportunity to provide input on the implementation of the California Consumer Privacy Act. Americans are increasingly worried about the security of their data and 85% say they want to control what data is collected about them. The CCPA is the first law in the nation to create privacy rights over our digital data, giving us the right to know what is being collected and the right to have that information deleted.

Your job is to make sure that the law is implemented in a way to ensure Californians get the level of protection intended by the act. The latest massive data breach by some of the nation's largest banks, which compromised 24 million financial documents for tens of thousands of loan and mortgage customers, illustrates why this rulemaking process is important. Everything an identity thief needs to impersonate a person and steal sensitive information was exposed in that breach. Similarly, Marriott disclosed a breach of 400 Million of its customers' records including passport numbers and credit cards. Facebook recently revealed another major breach of public trust, admitting that it gave major tech companies greater access to user data than they disclosed.

These breaches demonstrate the need for strong regulations and the right to sue when data is compromised to ensure companies are responsibly managing their customers' data. We would like to make the following recommendations as you begin the rulemaking process:

Financial Incentives

Rules to ensure that companies do not discriminate against those who prefer to have their data private are critical. The CCPA clearly states the intent to ensure: "The right of Californians to equal service and price, even if they exercise their privacy rights." Section 125(b)4 says any financial incentive dreamt up by a company to convince a consumer to allow it to sell their data cannot be "unjust, unreasonable, coercive or usurious."

The law allows businesses to offer financial incentives to convince consumers not to opt out only if those incentives are related to the value of consumers' data. Any incentives provided by companies to convince consumers to allow data sales cannot force mid- and low-income consumers to give up their privacy in order to use a website or service. That means any different price or disparate level of service must be "directly related" to the value of a consumer's data.

When a consumer is offered a financial incentive to allow their data to be sold, the company must be explicit about how it is calculated and prove the charge is correlated to the value of a consumer's data. For example, if a blog site wants to offer the financial incentive of a free subscription in exchange for the right to sell a consumer's data, they should provide evidence that the consumer's data is worth the value of a subscription.

The best way for your office, and the public, to be confident that companies aren't discriminating against consumers who choose privacy, is to require disclosure of revenues and the method by which a company calculates value of the data. To that end, we urge you to require any company seeking to offer consumers incentives to allow their data to be shared to submit quarterly reports to your office on the revenue they bring in from the sale of consumer data, the number of consumers whose data they sell, and a per-user value of that data.

Companies must prove that any financial incentive is directly tied to the value of consumer data to ensure Californians' right to equal service and price under the CCPA.

Opting-Out

Companies must give consumers a clear and obvious way to opt out of having their data sold. We strongly recommend requiring companies to have a link or box that states, "DO NOT SELL OR SHARE MY PERSONAL INFORMATION." The text should be in a larger font than the predominant font size of the website, in a contrasting color, and clearly be a link/invitation for consumers to take action. The opt-out link should be available on every page of a website. This should be a simple process with clear language that avoids confusing legal terms. Companies should be prohibited from burying the opt-out beneath more than two click-throughs: One click to get to the page explaining what it means to opt out, and a second click to actually opt out.

Right to download data

The ability of the consumers to download their data, and move it to another service, is essential for individual control of their data. Despite industry complaints, this right has already been successfully implemented in Europe under the GDPR.

Unique identifiers

The CCPA is clear that an IP address is a unique identifier, and that “personal information” includes anything “capable of being associated with” or “reasonably be linked, directly or indirectly” with a household, consumer or family. There is no good justification for excluding IP address since it can easily be linked to a specific person or household.

Categories of information

Rules should protect all personal information collected by companies. The law defines “personal information” broadly as all data a company collects and relates to a person in any way. This category must not be limited to traditionally “sensitive” categories of data because the inferences companies can make from even seemingly innocuous data are broad.

Categories of information that a website must disclose to consumers should distinctly identify “Data About Your Activity On This Site” (and related sites): purchasing habits, number of hours or time of day a consumer is on a site, articles or products viewed, “likes”, and similar data categories. Companies must also disclose inferences they make about consumers based on that data:

If there is value to a company sharing or selling one’s data, there is a value to consumers opting out of its sale. Consumers who opt-out of data sales must also have their information protected.

Thank you for the opportunity to provide these recommendations towards ensuring a full and fair adoption of California’s landmark privacy act.

Sincerely,

Adam Scow, Consumer Advocate