Published on *The National Law Review* https://natlawreview.com

California Privacy Agency Extracts Civil Penalties in its First Settlement Not Involving Data Brokers

Article By:

Alan L. Friel

Kyle R. Fath

Niloufar Massachi

Companies in all industries take note: regulators are scrutinizing how companies offer and manage privacy rights requests and looking into the nature of vendor processing in connection with application of those requests. This includes applying the proper verification standards and how cookies are managed. Last week, the California Privacy Protection Agency ("CPPA" or "Agency") provided yet another example of this regulatory focus in its Stipulated Final Order ("Order") with automotive company, American Honda Motor Co., Inc. ("Honda").

The CPPA alleged that Honda violated the California Consumer Privacy Act ("CCPA") by:

- requiring Californians to verify themselves where verification is not required or permitted (the right to opt-out of sale/sharing and the right to limit) and provide excessive personal information to exercise privacy rights subject to verification (know, delete, correct);
- using an online cookie management tool (often known as a CMP) that failed to offer Californians their privacy choices in a symmetrical or equal way and was confusing;
- requiring Californians to verify that they gave their agents authority to make opt-out of sale/sharing and right to limit requests on their behalf; and
- sharing consumers' personal information with vendors, including ad tech companies, without having in place contracts that contain the necessary terms to protect privacy in connection with their role as either a service provider, contractor, or third party.

This Order illustrates the potential fines and financial risks associated with non-compliance with the state privacy laws. Of the $632,500 administrative fine lodged against the company, the Agency clearly spelled out that $382,500 of the fine accounts for 153 violations – *$2,500 per violation* – that are alleged to have occurred with respect to Honda's consumer privacy rights processing between July 1 and September 23, 2023. It is worth emphasizing that the Agency lodged the maximum administrative fine – "*up to* two thousand five hundred ($2,500)" – that is available to it for non-intentional violations for each of the incidents where consumer opt-out / limit rights were wrongly applying verification standards. It Is unclear to what the remaining $250,000 in fines were attributed,

but they are presumably for the other violations alleged in the order, such as disclosing PI to third parties without having contracts with the necessary terms, confusing cookie and other consumer privacy requests methods, and requiring excessive personal data to make a request. It is unclear the number of incidents that involved those infractions but based on likely web traffic and vendor data processing, the fines reflect only a fraction of the personal information processed in a manner alleged to be non-compliant.

The Agency and Office of the Attorney General of California (which enforces the CCPA alongside the Agency) have yet to seek truly jaw-dropping fines in amounts that have become common under the UK/EU General Data Protection Regulation ("GDPR"). However, this Order demonstrates California regulators' willingness to demand more than remediation. It is also significant that the Agency requires the maximum administrative penalty on a per-consumer basis for the clearest violations that resulted in denial of specific consumers' rights. This was a relatively modest number of consumers: "119 Consumers who were required to provide more information than necessary to submit their Requests to Opt-out of Sale/Sharing and Requests to Limit, 20 Consumers who had their Requests to Opt-out of Sale/Sharing and Requests to Limit denied because Honda required the Consumer to Verify themselves before processing the request, and 14 Consumers who were required to confirm with Honda directly that they had given their Authorized Agents permission to submit the Request to Opt-out of Sale/Sharing and Request to Limit on their behalf." The fines would have likely been greater if applied to all Consumers who accessed the cookie CMP, or that made requests to know, delete, or correct. Further, it is worth noting that many companies receive thousands of consumer requests per year (or even per month), and the statute of limitations for the Agency is five years; applying the per-consumer maximum fine could therefore result in astronomical fines for some companies.

Let us also not forget that regulators also have injunctive relief at their disposal. Although, the injunctive relief in this Order was effectively limited to fixing alleged deficiencies, it included "fencing in" requirements such as use of a UX designer to evaluate consumer request "methods – including identifying target user groups and performing testing activities, such as A/B testing, to access user behavior" – and reporting of consumer request metrics for five years. More drastic relief, such as disgorgement or prohibiting certain data or business practices, are also available. For instance, in a recent data broker case brought by the Agency, the business was barred from engaging in business as a data broker in California for three years.

We dive into each of the allegations in the present case further below and provide practical takeaways for in-house legal and privacy teams to consider.

Requiring consumers to provide more info than necessary to exercise verifiable requests and requiring verification of CCPA sale/share opt-out and sensitive PI limitation requests.

The Order alleges two main issues with Honda's rights request webform:

- Honda's webform required too many data points from consumers (e.g., first name, last name, address, city, state, zip code, email, phone number). The Agency contends that requiring all of this information necessitates that consumers provide more information than necessarily needed to exercise their verifiable rights considering that the Agency alleged that "Honda generally needs only two data points from the Consumer to identify the Consumer within its database." The CPPA and its regulations allow a business to seek additional personal

information if necessary to verify to the requisite degree of certainty required under the law (which varies depending on the nature of the request and the sensitivity of the data and potential harm of disclosure, deletion or change), or to reject the request and provide alternative rights responses that require lesser verification (e.g., treat a request of a copy of personal information as a right to know categories of person information). However, the regulations prohibit requiring more personal data than is necessary under the particular circumstances of a specific request. Proposed amendments the Section 7060 of the CCPA regulations also demonstrate the Agency's concern about requiring more information than is necessary to verify the consumer.
- Honda required consumers to verify their Requests to Opt-Out of Sale/Sharing and Requests to Limit, which the CCPA prohibits.

In addition to these two main issues, the Agency also alluded to (but did not directly state) that the consumer rights processes amounted to dark patterns (Para. 38). The CPPA cited to the policy reasons behind differential requirements as to Opt-Out of Sale/Sharing and Right to Limit; i.e., so that consumers can exercise Opt-Out of Sale/Sharing and Right to Limit requests without undue burden, in particular, because there is minimal or nonexistent potential harm to consumers if such requests are not verified.

In the Order, the CPPA goes on to require Honda to ensure that its personnel handling CCPA requests are trained on the CCPA's requirements for rights requests, which is an express obligation under the law, and confirming to the Agency that it has provided such training within 90 days of the Order's effective date.

Practical Takeaways

- Configure consumer rights processes, such as rights request webforms, to only require a consumer to provide the minimum information needed to initiate and verify (if permitted) the specific type of request. This may be difficult for companies that have developed their own webforms, but most privacy tech vendors that offer webforms and other consumer rights-specific products allow for customizability. If customizability is not possible, companies may have to implement processes to collect minimum information to initiate the request and follow up to seek additional personal information if necessary to meet CCPA verification standards as may be applicable to the specific consumer and the nature of the request.
- Do not require verification of do not sell/share and sensitive PI limitation requests (note, there are narrow fraud prevention exceptions here, though, that companies can and should consider in respect of processing Opt-Out of Sale/Sharing and Right to Limit requests).
- Train personnel handling CCPA requests (including those responsible for configuring rights request "channels") to properly intake and respond to them.
- Include instructions on how to make the various types of requests that are clear and understandable, and that track the what the law permits and requires.

Requiring consumers to directly confirm with Honda that they had given permission to their authorized agent to submit opt-out of sale/sharing sensitive PI limitation requests

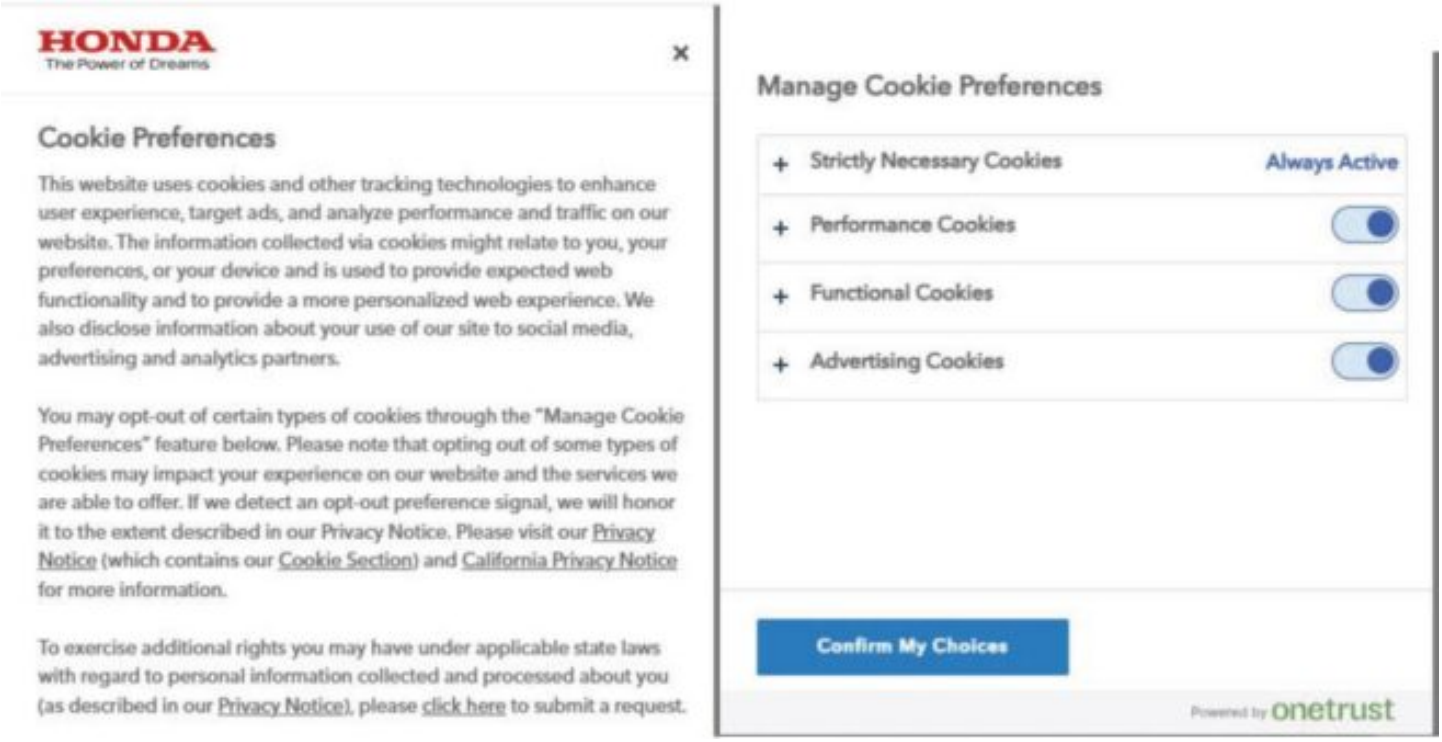
The CPPA's Order also outlines that Honda allegedly required consumers to directly confirm with Honda that they gave permission to an authorized agent to submit Opt-Out of Sale/Sharing and Right to Limit requests on their behalf. The Agency took issue with this because under the CCPA, such

direct confirmation with the consumer regarding authority of an agent is only permitted as to requests to delete, correct, and know.

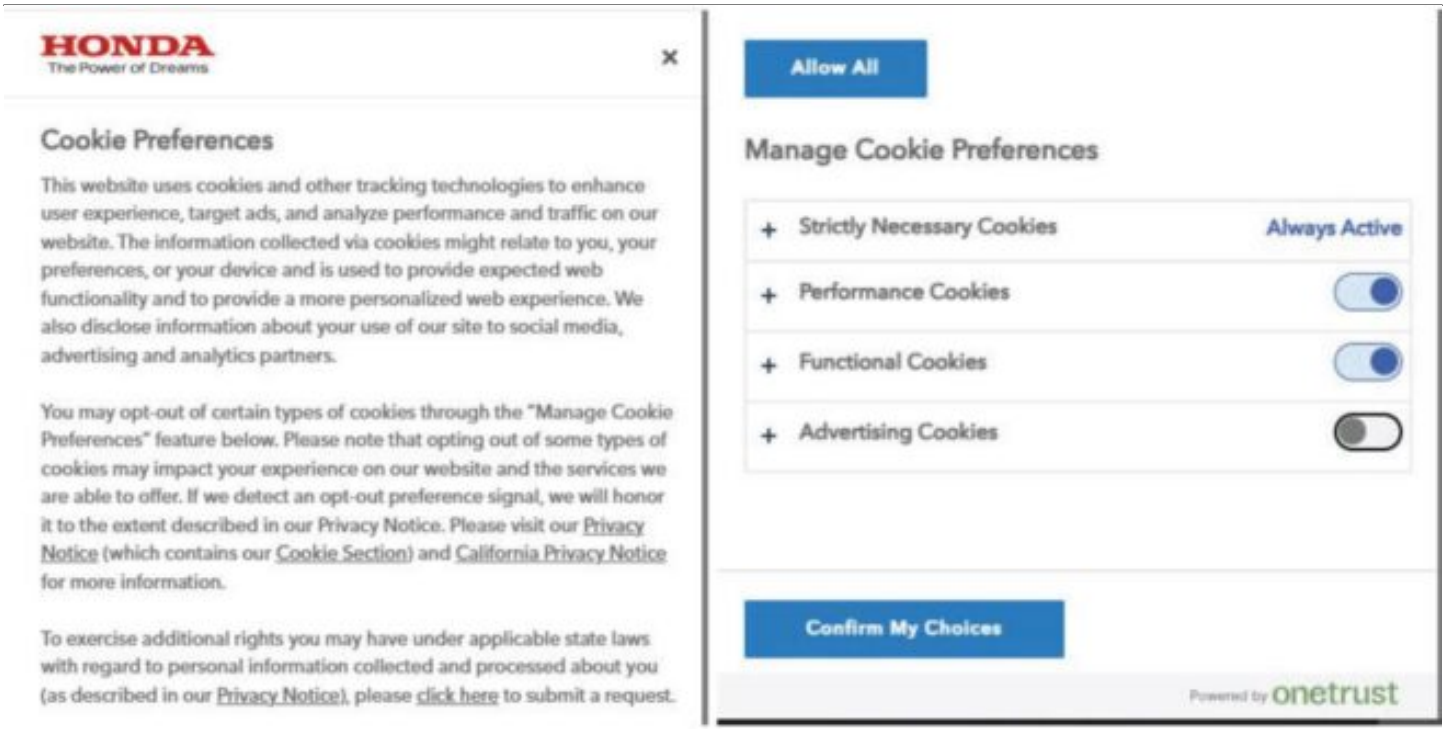
Practical Takeaways: When processing authorized agent requests to Opt-Out of Sale/Sharing or Right to Limit, avoid directly confirming with the consumer or verifying the identity of the authorized agent (the latter is also permitted in respect of requests to delete, correct, and know). Keep in mind that what agents may request, and agent authorization and verification standards, differ from state-to-state.

Failure to provide "symmetry in choice" in its cookie management tool

The Order alleges that, for a consumer to turn off advertising cookies on Honda's website (cookies which track consumer activity across different websites for cross-context behavioral advertising and therefore require an Opt-out of Sale/Sharing), consumers must complete two steps: (1) click the toggle button to the right of Advertising Cookies and (2) click the "Confirm My Choices" button," shown below:



The Order compares this opt-out process to that for opting back into advertising cookies following a prior opt-out. There, the Agency alleged that if consumers return to the cookie management tool (also known as a consent management platform or "CMP") after turning "off" advertising cookies, an "Allow All" choice appears (as shown in the below graphic). This is likely a standard configuration of the OneTrust CMP that can be modified to match the toggle and confirm approach used for opt-out. Thus, the CPPA alleged, consumers need only take one step to opt back into advertising cookies when two steps are needed to opt-out, in violation of and express requirement of the CCPA to have no more steps to opt-in than was required to opt-out.



The Agency took issue with this because the CCPA requires businesses to implement request methods that provide symmetry in choice, meaning the more privacy-protective option (e.g., opting-out) cannot be longer, more difficult, or more time consuming than the less privacy protective option (e.g., opting-in).

The Agency also addressed the need for symmetrical choice in the context of "website banners," also known as cookie banners, pointing to an example cited as insufficient symmetry in choice from the CCPA regulations – i.e., using "'Accept All' and 'More Information,' or 'Accept All' and 'Preferences' – is not equal or symmetrical" Because it suggests that the company is seeking and relying on consent (rather than opt-out) to cookies, and where consent is sought acceptance and acceptance must be equally as easy to choose. The CCPA further explained that "[a]n equal or symmetrical choice" in the context of a website banner seeking consent for cookies "could be between "Accept All" and "Decline All." Of course, under CCPA consent to even cookies that involve a Share/Sale is not required, but the Agency is making clear that where consent is sought there must be symmetry in acceptance and denial of consent.

The CPPA's Order also details other methods by which the company should modify its CCPA requests procedures including (i) separating the methods for submitting sale/share opt-out requests and sensitive PI limitation requests from verifiable consumer requests (e.g., requests to know, delete, and correct); (ii) including the link to manage cookie preferences within Honda's Privacy Policy, Privacy Center, and website footer; and (iii) applying global privacy control ("GPC") preference signals for opt-outs to known consumers consistent with CCPA requirements.

Practical Takeaways

- It is unclear whether the company configured the cookie management tool in this manner deliberately or if the choice of the "Allow All" button in the preference center was simply a matter of using a default configuration of the CMP, a common issue with CMPs that are built off of a (UK/EU) GDPR consent model. Companies should pay close attention to the configuration of their cookie management tools, including in both the cookie banner (or first layer), if used, and the preference center (shown above), and avoid using default settings and

configurations provided by providers that are inconsistent with state privacy laws. Doing so will help mitigate the risk of choice asymmetry presented in this case, and the risks discussed in the following three bullets.

- State privacy laws like the CCPA are not the only reason to pay close attention and engage in meticulous legal review of cookie banner and preference center language, and proper functionality and configuration of cookie management tools.
- Given the onslaught of demands and lawsuits from plaintiffs' firms under the California Invasion of Privacy Act and similar laws – based on cookies, pixels, and other tracking technologies – many companies turn to cookie banner and preference center language to establish an argument for a consent defense and therefore mitigate litigation risk. In doing so it is important to bear in mind the symmetry of choice requirements of state consumer privacy laws. One approach is to make it clear that acceptance is of the site terms and privacy practices, which include use of tracking by the operator and third parties, subject to the ability to opt-out of some types of cookies. This can help establish consent to use of cookies by use of the site after notice of cookie practices, while not suggesting that cookies are opt-in, and having lack of symmetry in choice.
- In addition, improper wording and configuration of cookie tools – such as providing an indication of an opt-in approach ("Accept Cookies") when cookies in fact already fired upon the user's site visit, or that "Reject All" opts the user out of all, including functional and necessary cookies that remain "on" after rejection – present risks under state unfair and deceptive acts and practices (UDAAP) and unfair competition laws, and make the cookie banner notice defense to CIPA claims potentially vulnerable since the cookies fire before the notice is given.
- Address CCPA requirements for GPC, linking to the business's cookie preference center, and separating methods for exercising verifiable vs. non-verifiable requests. Where the business can tie a GPC signal to other consumer data (e.g., the account of a logged in user), it must also apply the opt-out to all linkable personal information.
- Strive for clear and understandable language that explains what options are available and the limitations of those options, including cross-linking between the CMP for cookie opt-outs and the main privacy rights request intake for non-cookie privacy rights, and explain and link to both in the privacy policy or notice.
- Make sure that the "Your Privacy Choices" or "Do Not Sell or Share My Personal Information" link gets the consumer to both methods. Also make sure the opt-out process is designed so that the required number of steps to make those opt-outs is not more than to opt-back in. For example, linking first to the CMP, which then links the consumer rights form or portal, rather than the other way around, is more likely to avoid the issue with additional steps just discussed.

Failure to produce contracts with advertising technology companies

The Agency's Order goes on to allege that Honda did not produce contracts with advertising technology companies despite collecting and selling/sharing PI via cookies on its website to/with these third parties. The CPPA took issue with this because the CCPA requires a written contract meeting certain requirements to be in place between a business and PI recipients that are a CCPA service provider, contractor, or third party in relation to the business. We have seen regulators request copies of contracts with *all* data recipients in other enforcement inquiries.

Practical Takeaways

- Vendor and contract management are a growing priority of privacy regulators, in California

and beyond, and should be a priority for all companies. Be prepared to show that you have properly categorized all personal data recipients, and have implemented and maintain processes to ensure proper contracting practices with vendors, partners, and other data recipients, which should include a diligence and assessment process to ensure that the proper contractual language is in place with the data recipient based on the recipient's data processing role. To state it another way, it may not be proper as to certain vendors to simply put in place a data processing agreement or addendum with service provider/processor language. For instance, vendors that process for cross-context behavioral advertising cannot qualify as a service provider/contractor. In order to correctly categorize cookie and other vendors as subject to opt-out or not, this determination is necessary.

- Attention to contracting is important under the CCPA in particular because different language is required depending on whether the data recipient constitutes a "third party," "service provider," or a "contractor," the CCPA requires different contracting terms be included in the agreements with each of those three types of personal information recipients. Further, in California, the failure to have all of the required service provider/contractor contract terms will convert the recipient to a third party and the disclosure into a sale.

Conclusion

This case demonstrates the need for businesses to review their privacy policies and notices, and audit their privacy rights methods and procedures to ensure that they are in compliance with applicable state privacy laws, which have some material differences from state-to-state. We are aware of enforcement actions in progress not only in California, but other states including Oregon, Texas, and Connecticut, and these states are looking for clarity as to what specific rights their residents have and how to exercise them. Further, it can be expected that regulators will start looking beyond obvious notice and rights request program errors to data knowledge and management, risk assessment, minimization, and purpose and retention limitation obligations. Compliance with those requirements requires going beyond "check the box" compliance as to public facing privacy program elements and to the need to have a mature, comprehensive and meaningful information governance program.

National Law Review, Volume XV, Number 80