CLIENT ALERTS & INSIGHTS

First Civil Penalties Under the CCPA Through $1.2 Million Settlement For Cookie "Sale" Violations

SEPTEMBER 7, 2022

The enforcement marks a step-up in scrutiny and enforcement as new amendments to the CCPA are set to come into force Jan. 1, 2023 and as enforcement moves from the CA Attorney General to the new California Privacy Protection Agency. In late August 2022, the California Attorney General obtained the first court order enforcement of a California Consumer Privacy Act ("**CCPA**") settlement under its CCPA enforcement authority.

The $1.2 million settlement, set forth in a filed complaint and final judgement in California Superior Court, is the first instance of CCPA enforcement in the law's over four year history that the Attorney General has used the courts to impose civil penalties and obligations. The process is much akin to the FTC's consent decree power whereby it uses the federal courts to enter in final judgements and settlements for unfair and deceptive business practices.

It will also likely be the Attorney General's last instance of utilizing its CCPA enforcement power under the CCPA as the California Privacy Rights Act (passed via referendum in 2020) comes into effect Jan. 1, 2023, and transfers enforcement power to the new California Privacy Protection Agency.

The bulk of the alleged violations deal with the CCPA's requirements to allow users the ability to opt-out of the sale of their personal information. Specifically, the complaint and final judgement indicate that the Attorney General found that the use of advertising and analytics cookies on the business's website constituted a "sale."

Cookies have come under increasing scrutiny as of late especially in Europe, where the General Data Protection Regulation ("**GDPR**") requires a business to obtain an individual's prior written consent before using non-essential cookies on a website.

However, it is important to note that note all kinds of cookies are under increased scrutiny or increased regulation. Prior consent (under the GDPR) is not required for essential or operationally necessary cookies; and likewise, such cookies do not require businesses to provide consumers with an opt-out (under the CCPA). These cookies include those that are required for the operation of a given website and could include those needed make a "shopping cart" function work and those used to provide security or prevent fraud.

The cookies at issue in this case, and that are also under increased scrutiny, are cookies that are shared with third parties and for purposes beyond those required to make a website function. The most common of these non-essential cookies include analytics and advertising cookies.

CCPA "Sale" Standards and Requirements

Under the CCPA, a business that sells a consumer's personal information must give consumers the ability to opt-out of the sale of their personal information to third parties.

"Sell" is broadly defined as to capture both instances where the information is sold for monetary value, and instances where it is not sold for monetary value. Specifically, "selling" personal information includes any instance of selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal information to another business for any form of value.

Importantly, this includes where personal information is provided to a third party in exchange for a service being provided. There is a "service provider" exception that allows the transfer of personal information without that transfer being considered a sale.

The opt-out requirements *do not* apply where the business provides personal information to a service provider where the transfer of personal information is necessary for a business purpose and where (i) the business provides notice that the information is used and shared in this manner (e.g., through the website privacy policy); and (ii) the service provider does not further collect, sell, or use the personal information except as necessary for the applicable business purpose.

To meet these requirements, the CCPA requires a business to enter into a written contract with the service provider to ensure all parties commit to the foregoing obligations (i.e., no further collection, using, disclosing, sharing, or other processing of the personal information).

If there is not a written agreement in place between the parties implementing restrictions on subsequent use of the personal information involved, the transfer of personal data is considered a sale and the business must provide consumers the opt-out right.

Cookies Under Scrutiny

It is important to note that cookies are considered personal information under the CCPA. The definition of personal information includes any information that identifies, relates to, or that could be reasonably linked to (directly or indirectly) to a consumer. Unique Personal Identifiers fall within the definition of personal information.

A "Unique Personal Identifier" includes any persistent identifier that can be used to recognize or related to a consumer or household. This includes IP addresses, cookies, beacons, pixel tags, mobile ad identifiers, and other similar information.

In the Attorney General's complaint and final judgement obtained through the California Superior Court, the business was alleged to have been using third party analytics and advertising services on its website. Those third parties placed analytics and advertising cookies on the website; a very common practice.

The Attorney General alleged that the business's relationship with the various third parties constituted a "sale" because the business "gave companies access to consumer personal information in exchange for free or discounted analytics and advertising benefits"-highlighting the broad interpretation of "sale under the CCPA.

The complaint and final judgement also allege that written contracts or agreements were not in place that restricted the third party providers' further use, processing, sale, or transfer of the personal information collected via the cookies. Further, the business was not offering consumer the ability to opt-out of such transfers of personal information nor was it honoring Global Privacy Controls (controls consumers can implement to broadly opt-out where allowed).

Meaning, that the analytics and advertising cookies did not fall within the "service provider" exception, and further, that the business was in violation of the CCPA's opt-out requirements.

Fines and Penalties

The CCPA allows the Attorney General to seek fines of up to $2,500 per violation and up to $7,500 per intentional violation. Due to the number of violations alleged, the Attorney General was able to obtain the $1.2 million settlement.

Beyond the monetary fines, though, the settlement also includes affirmative obligations the business must meet.

Under the settlement, the business must, within 180 days and for 2 years thereafter (i) implement and maintain a program to assess and monitor its effectiveness of processing opt-out requests and compliance with Global Privacy Controls and (ii) conduct annual reviews of its website and mobile applications to determine what third parties collected personal information is shared with.

The annual reviews must be recorded and publicly disclosed.

As new data protection laws, rules, and regulations come into force both at the state and federal level, and as enforcement proceedings increase, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.