Alphabet Soup: Practical Advice on CPRA Obligations and Enforcement

Wynter Deagle
Sheppard Mullin

Orson Lucas
KPMG

Andy Medlin
Hot Topic

Sephora Complaint and Cure Letter

PEOPLE OF THE STATE OF CALIFORNIA,

Plaintiff,

v.

SEPHORA USA, INC.

Defendant.

Case No.

COMPLAINT FOR INJUNCTION, CIVIL PENALTIES, AND OTHER EQUITABLE RELIEF

(CIVIL CODE, § 1798.155 & BUSINESS AND PROFESSIONS CODE, § 17206)

12. Sephora's decision to provide third parties including "advertising networks, business partners, [and] data analytics providers" with access to its customers' data in exchange for services from those entities was a sale of personal information as defined by the CCPA. Section 1798.140, subdivision (t), broadly defines sales as the exchange of personal information for anything of value. Sephora's relationships with these third parties met that definition, because Sephora gave companies access to consumer personal information in exchange for free or discounted analytics and advertising benefits. For example, Sephora installed one widely-used analytics and advertising software package that let the analytics provider gather and keep personal information about an online shopper's activities. The analytics provider then gave Sephora data about what shoppers did on its website or in its app, like how many people looked at a particular product. The analytics provider also would determine who the shopper was, using extensive data gathered from other sources, and then present Sephora with the valuable option to serve targeted advertisements to the same shopper on the analytics provider's advertising network. Both the trade of personal information for analytics and the trade of personal information for an advertising option constituted sales under the CCPA.

State of the Union

14. In June 2021, the Attorney General commenced an enforcement sweep of large retailers to determine whether they continued to sell personal information when a consumer signaled an opt-out via the GPC. In part, the testing and investigation used commercially available browser extensions to monitor network traffic involving third-party advertising and analytics providers, and analyzed how that traffic changed when the GPC sent its "do not sell" signal. In investigating Sephora's website, the Attorney General found that activating the GPC had no effect and that data continued to flow to third-party companies, including advertising and analytics providers. Subsequent testing confirmed that Sephora's website took no action to block the transmission of personal information even when a California consumer signaled their opt-out using the GPC. In short, Sephora completely ignored the GPC.

AG Press Release: "I hope today's settlement sends a strong message to businesses that are still failing to comply with California's consumer privacy law. My office is watching, and we will hold you accountable. It's been more than two years since the CCPA went into effect, and businesses' right to avoid liability by curing their CCPA violations after they are caught is expiring. There are no more excuses. Follow the law, do right by consumers, and process opt-out requests made via user-enabled global privacy controls."

Cure Letter

CORPORATION SERVICE COMPANY
WHICH WILL DO BUSINESS IN
CALIFORNIA AS CSC - LAWYERS
INCORPORATING SERVICE
2710 Gateway Oaks Dr, Ste 150N
Sacramento, CA 95833

RE: CCPA Notice of Violations

Dear Sir/Madam:

The California Attorney General's Office writes to notify ▆▆▆▆▆▆▆ (hereinafter "BUSINESS"), of alleged violations of the California Consumer Privacy Act of 2018, Civil Code, § 1798.100 *et seq.* ("CCPA"), specifically, BUSINESS's failure to honor a consumer's opt out of sales as signaled by a global privacy control. This letter constitutes notice under § 1798.155 and triggers the 30-day period before an enforcement action may be filed. This notice applies to any corporate affiliates that share common branding. The Attorney General shall retest BUSINESS's website in 60 days to determine if BUSINESS has come into compliance, in addition to making any other appropriate investigation. If continued violations are discovered at that point, we may inform BUSINESS that it appears to still have an actionable violation, ask for a response, or initiate an investigation under Government Code section 11180 *et seq.*

Summary of the Violations

(1) Civil Code, § 1798.120, subd. (a); Cal. Code Reg., tit. 11, § 999.315, subd. (c)

BUSINESS appears to be selling personal information of opted-out consumers. The CCPA vests California consumers with "the right, at any time," to opt out of the sale of their personal information. (Civ. Code, § 1798.120, subd. (a).) Businesses must honor such opt outs and refrain from selling personal information that they collect. (*Id.*, § 1798.135, subd. (a)(4).) Sales are broadly defined as disclosing or making available consumers' personal information to third parties for anything of value. (*Id.*, § 1798.140, subd. (t).) Unless exempted, "sale" may include trading access to consumers' online activities in exchange for free, discounted, or improved advertising or analytics services and ad targeting options.

To facilitate the submission of a consumer's right to opt out of sales, particularly in the context of online requests, the CCPA's implementing regulations require business to process a universal opt-out signal or "global privacy control." Specifically, section 7026 requires that if "a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer." (Cal. Code Regs., tit. 11, § 7026, subd. (c).) For over a year, consumers have been able to signal such an opt-out using the aptly named "Global Privacy Control" ("GPC") available in certain browsers and extensions.

Preliminary investigation reveals that BUSINESS appears to be selling personal information despite consumers sending BUSINESS the GPC. The Attorney General tested BUSINESS's website using a GPC and BUSINESS continued to allow personal information to be made available to third parties providing advertising or analytics services. This appears to include circumstances where the third party is not a "Service Provider" under the CCPA and no other exception to sale appears to apply. For example, the Attorney General observed third party analytics providers attributing online activities to consumer-level user accounts accessed with the same IP address, even while the GPC was being broadcast. In doing so, BUSINESS appears to be ignoring valid opt-out requests and unlawfully selling personal information third parties.

Implications and Actions

Key Obligations and Areas of Focus

- Opt-out of sale or sharing for targeted advertising
- Opt-out preferences
- Data Minimization
- Consent
- Scanning sites for "low hanging fruit"
- Third party relationships

Immediate Actions

- Web portfolio inventory
- Cookie categorization
- Opt-out / preference banner (and supporting business processes)
- GPC enablement
- Google Restricted Data Processing (RDP) / Facebook Pixel Limited Data Usage (LDU) settings
- Testing and validation
- Contract review
- Update privacy notices

Future Enforcement

- Elimination of the cure period
- Dual enforcement
- Continued focus on websites user experience
- Execution of Consumer Rights
- Invitation for Preliminary Comments

§ 7025. Opt-Out Preference Signals.

(a) The purpose of an opt-out preference signal is to provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt-out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.

(b) A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

   (1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.

   (2) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

   (1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device, and, if known, for the consumer. This is not required for a business that does not sell or share personal information.

Litigation Trends

Website Tools

- Entities collect information about the interaction of consumers with websites to improve such services and to offer additional and related services.
- Meta Pixel: captures and shares certain types of information about consumers' interaction with specific websites.
- Session replay software: monitors specific consumer interactions (mouse clicks, keyboard strokes, video activity, or cursor movements).
- Chatbots: use artificial intelligence tools to assist and guide consumers who interact with certain websites.
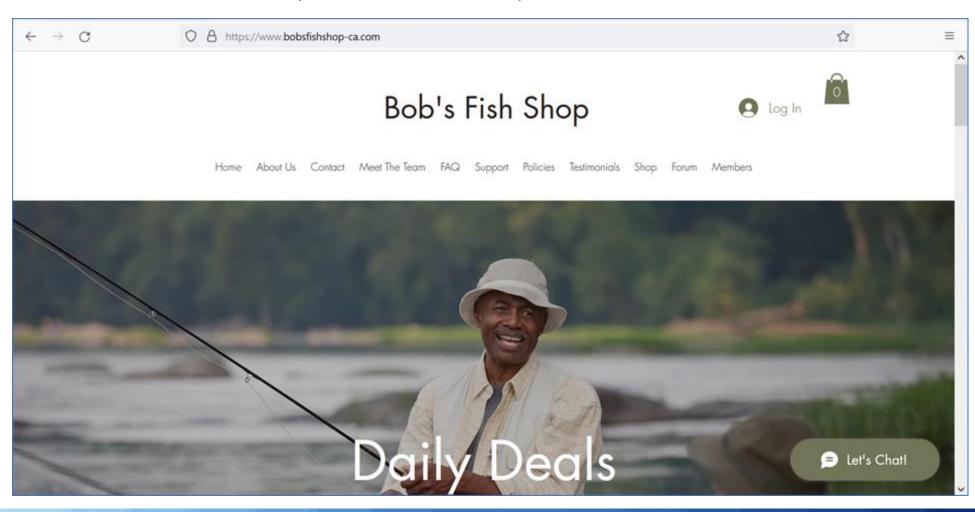
Types of Claims

- Federal and state anti-wiretapping laws
- Negligent misrepresentation
- Intrusion upon seclusion
- Invasion of privacy (CIPA)
- Breach of contract
- breach of fiduciary duty
- Video Privacy Protection Act

Litigation Avoidance

Know	What the website collects, how it is collected, for what purpose, and with whom it is shared
Ensure	Contracts with third-parties services used to improve the website and user experience or commercialize the collected data address data ownership, data privacy and data security concerns
Consider	Whether consent, and what format of consent, is necessary for processing activities.
Understand	The options for modifying data collection and processing (GPC, RDP, LDU etc.)
Update	Website privacy policies and terms and conditions to provide clear and accurate disclosures, include resources required for state-specific compliance (such as CCPA), include enforceable terms, and satisfy consent requirements (including hyperlinks)

Putting It Into Practice

https://www.bobsfishshop-ca.com/

Data Collection

Contact Support

How Can We Help?

First Name

Last Name

Email

Phone

Choose an Issue ⌄

Let us know what you need help with...

Get in Touch

Get in Touch

104 Main St, San Francisco, CA 94105, USA

jwcolliii@yahoo.com

8008675309

Let's Chat!

Name *

Enter your name

Email *

Enter your email

Phone

Enter your phone number

Address

Enter your address
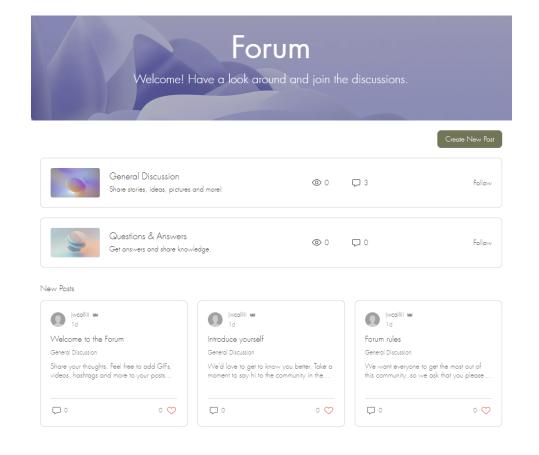
Subject

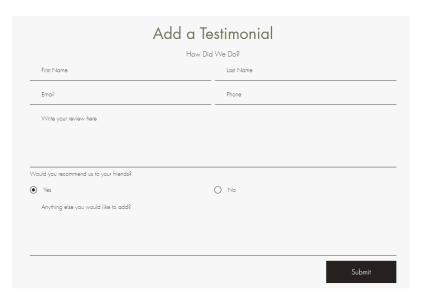Type the subject

Message

Type your message here...

Submit

Subscribe Form

e.g., email@example.com   Join

Data Collection

Cookies

Cookie	Domain	Description	Duration	Type
ssr-caching	www.bobsfishshop-ca.com	The ssr-caching cookie is set by WIX and indicates how a site was rendered.	past	Necessary
XSRF-TOKEN	.www.bobsfishshop-ca.com	This cookie is set by Wix and is used for security purposes.	session	Necessary
hs	.www.bobsfishshop-ca.com	Wix platform sets this cookie for security purposes.	session	Necessary
svSession	.www.bobsfishshop-ca.com	Wix platform sets this cookie to identify unique visitors and track a visitor's session on a site.	2 years	Necessary
bSession	.www.bobsfishshop-ca.com	No description available.	30 minutes	Other
fedops.logger.defaultOverrides	www.bobsfishshop-ca.com	No description	1 minute	Other

Opt-Outs

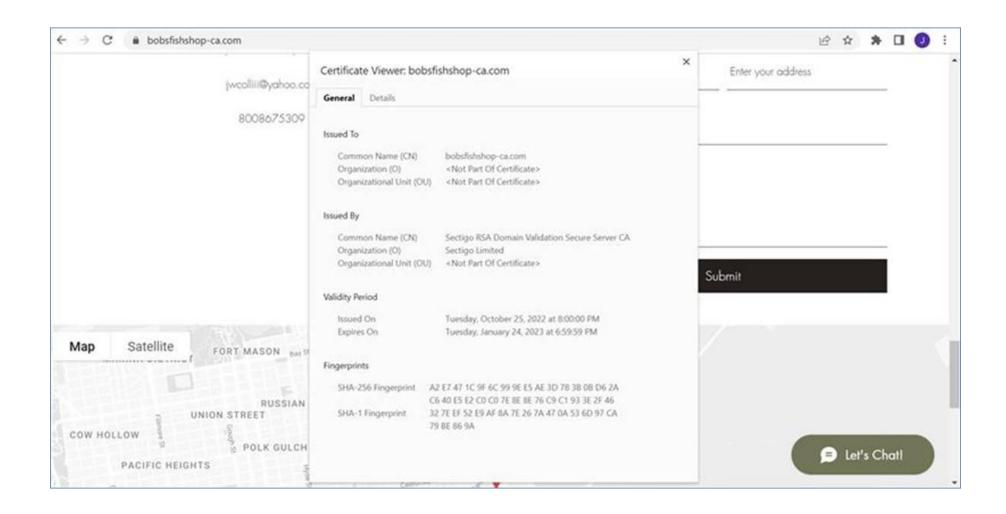## Bob's Fish Shop

Log In

Home   About Us   Contact   Meet The Team   FAQ   Support   Policies   Testimonials   Shop   Forum   Members

Opt-out is available at purchase in the event a user does not want to have their meta data collected or used for any marketing efforts.

Privacy Policy

Security

Questions & Contacts

Wynter Deagle

wdeagle@sheppardmullin.com
o: 858-720-8947
m: 401-439-0143
https://www.linkedin.com/in/wynterlavier/

Andy Medlin

amedlin@hottopic.com
o: 626-667-3600
https://www.linkedin.com/in/phillip-medlin-b1696858//

Orson Lucas

olucas@kpmg.com
m: 704-502-1067
https://www.linkedin.com/in/orsonlucas/