

# LEGAL CONSIDERATIONS FOR THE USE OF ABANDONMENT AUTOMATED EMAIL MARKETING AGAINST THE BACKDROP OF CAN-SPAM AND CPRA

*Disclaimer: This document is for informational purposes only. The information communicated herein is not intended to constitute legal advice. Nor is this document intended to be an exhaustive description of all relevant requirements. For example, while we discuss Federal and California law we don't provide a nationwide legal survey. Please consult your own legal counsel with any questions.*

The goal of this document is to discuss the U.S. legal context relating to use of a technology platform (hereinafter referred to as “Platform”) capable of gleaning email addresses of visitors to websites who have not shared their email address directly with the website owner. The Platform sends automated abandonment emails only to website visitors it can identify that have provided consent to the Platform provider or a partner of the Platform provider on a different site.

We start with our conclusions but please feel free to read on for additional context.

## **Primary conclusions regarding CAN-SPAM Act restrictions as to Platform usage:**

- The CAN-SPAM Act is national law that sets the rules for commercial email. The FTC revisited its applicability as recent as 2019 and confirmed that the law was still appropriate as written.
- Consistent with the Act, Platform users can send emails to email addresses acquired via the Platform provided that recipients have not previously opted-out to receiving marketing emails from the Platform user. The Platform satisfies this requirement because it is designed to automatically preclude emails from being sent to opted-out visitors.
- The Platform should not collect or provide email addresses to users of the Platform if those email addresses were acquired from a website that prohibits email address harvesting. This is readily achieved by updating your policies and/or consents as necessary.

-All emails sent via the Platform are required to include an unsubscribe link or other opt-out mechanism, and Platform users should promptly honor all opt-out requests. The Platform service satisfies this by ensuring that all emails sent include an unsubscribe link. Users facilitate compliance by honoring all opt-out requests they may receive.

## **Primary conclusions regarding California's CPRA restrictions as to Platform usage:**

- CPRA doesn't apply to every business. See below categories of applicability.
- Even if CPRA does apply to you, use of the Platform to acquire email addresses and send emails to those addresses remains permissible so long as users provide the required notice and the ability to opt-out of such sharing. This is readily achieved by updating your policies and/or consents as necessary, and providing the ability to opt-out.

## CAN-SPAM SUMMARY

The Federal Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003, also known as the [CAN-SPAM Act](#), is national law that sets the rules for commercial email. This law is intended to apply to companies that send emails whose primary purpose is to advertise or promote a commercial product or service. Per the Act, a “transactional or relationship message” may not contain false or misleading routing information, but otherwise is exempt from most provisions of the Act.

In other words, the Act does not preclude sending commercial emails without receipt of prior express consent or opt-in as long as the email includes an opt-out or unsubscribe link and meets some other basic requirements listed below. See Federal Trade Compliance (FTC) guidance regarding the Act [here](#).

An example of a “transactional or relationship message” is as an email that facilitates a transaction or updates an

existing customer, e.g., as to warranty information or a customer's outstanding balance, etc.

In addition to the above, the Act generally requires the following:

***-Don't email visitors that have opted-out or unsubscribed.***

***-Don't use deceptive subject lines.***

***-Don't use false or misleading header information.***

Your "From," "To," "Reply-To," and routing information must be accurate.

***-Identify the message as an ad.***

***-Tell recipients where you're located.***

***-Tell recipients how to opt out of receiving future email from you and honor opt-out requests promptly.***

***-Monitor what others are doing on your behalf. Even if you hire another company to handle your email marketing, you can't contract away your legal responsibility to comply with the law.***

In 2019, the FTC reviewed the Act and accepted public comments in order to determine whether the law was still

appropriate as written. On February 12, 2019, [the FTC confirmed](#) that the Act does not require that recipients affirmatively consent or opt-in to receiving commercial emails. Rather, each email must contain a clear and conspicuous notice the recipient can opt-out of receiving more commercial email from the sender.

## **CALIFORNIA PRIVACY LAW SUMMARY**

### **California Privacy Rights Act (CPRA) amending the California Consumer Privacy Act (CCPA)**

The [CPRA](#), a ballot initiative passed by voters in November 2020, amends the CCPA and renames the CCPA to the CPRA. The CPRA includes additional privacy protections for consumers as discussed below.

If you collect personal information from residents of the State of California while they are in California you are likely doing business in California and CPRA likely applies to you.

## **Opt-Out of Sharing for Targeted Advertising:**

The CPRA extends a consumer's right to opt-out of sales to include a right to opt-out of the sharing of the consumer's personal information for targeted advertising.

The CPRA contains an opt-out requirement for the sharing or sales of personal information, with the exception of the sharing or sales of personal information relating to children under the age of 16.

The CPRA does not outright prohibit the sharing of personal information. Rather, if a company shares personal information for targeted advertising the company must provide notice of this to the consumer and give the consumer at least two (2) methods for opting-out of the sharing of personal information for targeted advertising, one of which must be an interactive webform able to accept opt-out requests.

## **CPRA Notice:**

One of the primary requirements of the CPRA is to provide a "Do Not Sell or Share My Personal Information" and a

privacy notice or privacy policy to website visitors complying with the requirements of the CPRA.

With respect to the Platform generally speaking, the CPRA requires notice to website visitors if personal information that identifies or can be reasonably used to identify them is collected by the website owner, for the purposes for collecting, selling, or sharing the personal information.

### ***Does the CPRA apply to your business?***

The CPRA applies to any business, i.e., a for-profit legal entity, that collects and sells consumer “personal information,” with a few exemptions detailed in the CPRA. The California law sets a floor in terms of revenue and the number of consumer records being processed for the CPRA to apply.

A company has to meet one or more of the following for the CPRA to apply:

- Have \$25 million or more in annual revenue (not limited to revenue generated in or from California); or

- Annually buys, sells or shares personal information of 100,000 or more California consumers or households; or
- Earn more than half of its annual revenue selling or sharing consumers' personal data.

### ***Do you need to revise your privacy policies?***

The CPRA has added several new substantive elements to the required disclosures that must be included in a privacy notice or policy.

In addition to the information that must be included under the existing California laws or provided pursuant to California's "Shine the Light" law, online privacy policies must include:

- A description of a consumers' rights under the CPRA.
- A description of the categories of personal information collected by the business in the preceding 12 months.
- The commercial and business purposes for which the personal information is collected.
- The categories of personal information sold or disclosed

for a business purpose in the preceding 12 months.

-The categories of third-parties with which personal information is shared.

-If the Company sells or shares personal information, a link to a “Do Not Sell or Share My Personal Information” web-based opt-out link.

-A description of any financial incentives for providing data or not exercising rights.