POSSIBLENOW®
Marketing Compliance Made Simple

The Opt Out Mistakes Costing Companies Money

Twenty U.S. states now have their own comprehensive data privacy laws, with more under consideration and discussion. Businesses across many industries, including automotive, media, app development, and retail, have found themselves on the wrong end of these enforcement actions.

A common theme in these penalties is opt-out functionality on websites and apps. The law requires businesses to provide consumers with an easy way to opt out of the sale or sharing of their personal data and the use of web trackers.

Apps Without Opt-Out Functionality

Many state privacy laws require businesses to provide an opt-out mechanism that reflects how the business interacts with the consumer. This means companies with apps must provide users with a way to opt out within their apps.

Examples of Violations:

- **Jam City,** a mobile gaming company, paid a $1.4 million settlement for violating the CCPA. An investigation found that Jam City did not provide a CCPA-compliant opt-out link within its apps. 20 of Jam City's 21 apps did not provide an option to opt out of the sale and sharing of personal information. One of Jam City's apps had a "Data Privacy" link, but it did not reference the CCPA and did not clearly state if it would stop the sale or sharing of personal information.

- The majority of **Sling TV** customers access the platform through an app on devices such as their smart television or gaming console. The app did not provide users with an easy-to-use avenue to opt out. Instead, they had to use a long URL in a web browser, usually on a different device. Sling TV was fined $530,000 for this and other violations.

Banners Missing a Decline Button

Notice banners that appear on websites and apps informing users and visitors about the collection and use of personal data must include a "Decline" or opt-out button. Forcing users to click "Agree" to close the banner is a violation.

Example Violation:

- **PlayOn** is a company that designs platforms for high schools to sell and manage digital tickets, stream events, track scores, player bios, stats, etc. The notice banners on its websites required consumers to click "Agree" to the use of tracking technologies and provided no other way to close the notice banner.

  When using PlayOn's GoFan ticketing platform on a mobile device, the notice banner covered the portion of the screen that allowed consumers to redeem their ticket. This forced consumers to click "Agree" on the notice banner before they could use their tickets.
  These violations were a part of PlayOn's $1.1 million fine.

Requiring Users to Verify Their ID or Email

The CCPA and many other state privacy laws prohibit businesses from requiring identity verification, such as email confirmation, as a condition of opting out of the sale or sharing of personal information. To avoid creating "unnecessary friction," businesses are only allowed to ask for information strictly necessary to honor the opt-out request.

Examples of Violations:

- **Ford** provided an interactive form for consumers to opt out of the sale/sharing of their data on its website. The form captured enough information for Ford to process the request, but Ford displayed a message directing consumers to check their "email for confirmation." The company then sent an email telling consumers it had received the request, but before completion, they must confirm their email and identity by clicking a button.

  Ford further explained that "Once we have confirmed your identity," it would "respond to your request within the legally required time period." If a consumer did not click "Confirm Email," Ford deemed their request as "expired." This resulted in Ford not processing dozens of opt-outs within the timeframe (15 business days) required by the CCPA. The email verification process was a major factor in Ford's $375,000 settlement.

- **Honda's** "Submit a Privacy Request" link took consumers to a "Consumer Privacy Rights Request Form" that required the same information for five different requests: Do Not Sell or Share My Personal Information, Limit Use of My Sensitive Personal Information, Opt-Out of Automated Decision Making and Profiling, and Delete My Personal Information.

- Honda required consumers to provide their first name, last name, address, city, state, zip code, preferred method to receive updates, email, and phone number to submit the request. Under many state privacy laws, opting out does not obligate consumers to verify their identity. Honda was fined $632,500 for this and other violations.

- **Todd Snyder's** privacy policy included a link to a Privacy Portal where consumers could submit CCPA requests. People were redirected to a Data Request Form that allowed them to select a request type, including "Do Not Sell or Share to a Third Party."

  Regardless of the selected request type, the Data Request Form required consumers to provide their first and last name, email, country of residence, and a photograph of the consumer holding their "identity document." Under the CCPA, government identification (driver's license, passport, etc.) is considered sensitive personal information. Todd Snyder was fined $345k.

Failing to Honor Opt-Outs Across All Platforms

Businesses that operate multiple platforms must honor opt-out requests on all platforms. If a logged-in user opts out of tracking or sharing on platform A, that opt-out must also apply when the user is using platform B.

Example Violation:

- A **major streaming platform** paid a $2.75 million settlement for various violations, including failing to apply opt-outs across platforms. The company operates a bundle of streaming services, where consumers could use the same login information for all three. Under setup, consumers could only fully opt out if they completedthe company's opt-out web form and used the opt-out toggle for each service on each device the consumer used. For customers with the bundle, this means they may have had to express their opt-out choice up to ten times.

Links Must Provide Easy Opt-Out Options - Not Just Instructions to Call or Email

A business that sells or shares personal information must also provide Notice of Right to Opt-out of Sale/Sharing by either posting a "Do Not Sell or Share My Personal Information" or "Your Privacy Choices" link on its websites. The link must either take consumers to a webpage that provides an easy opt-out method or immediately recognize the opt-out.

Examples of Violations:

- **PlayOn's** "Your Privacy Choices" link directed consumers to call or email PlayOn to place an opt-out request.

- **Jam City** also did not provide a compliant opt-out link on its website. The only opt-out rights mentioned on the website were found under a section titled "Cookies and Interest Based Advertising." There, consumers were told they could email Jam City to stop targeting advertising.

- **Tractor Supply** provided a "Do Not Sell My Personal Information" link in its website footer, which directed consumers to a web form. This form didn't give consumers the ability to opt out of sale/sharing with third-party trackers or inform them how to opt out. Tractor Supply was fined $1.3 million.

Opting In Takes More Steps than Opting Out

Many state privacy laws have a "Symmetry Rule," meaning the number of steps to opt-out must be the same as or fewer than the steps to opt-in.

Examples of Violations:

- The cookie management tool on **Honda's** website gave consumers the ability to opt out of targeted advertising and tracking. The cookies identified in their cookie management tool were "allowed" or "active" by default.

  To turn off the Advertising Cookies, consumers had to complete two tasks: toggling the button off and clicking the "Confirm My Choices" button. Consumers could opt back into Advertising Cookies in one step by clicking the "Allow All" button. This resulted in an asymmetrical choice.

Contact Us

(800) 585-4888 or (770) 255-1020

email | info@possiblenow.com

visit | www.possiblenow.com