

Inbox Overload: Massachusetts Lawsuits Target Online Retailers' Email Collection

Article By:

Taylor Ey

William Carter, CIPP/US

The [Massachusetts' Consumer Privacy in Commercial Transactions Act](#) (the "Act") limits companies' ability to request and collect personal identification information ("PII") that is not required for a transaction. The Act does not mention ecommerce and predated online retail, but, like many privacy litigation trends, this privacy law is now being tested in the online context. The Act gives a private right of action and has statutory damages of \$25 per violation (and a knowing violation of the Act permits recovery of up to three times the statutory amount).

What can we learn from these filings?

Plaintiffs are watching online data collection practices, even those that are pervasive. In these Massachusetts cases, the plaintiffs examine the consumer experience at checkout, looking at each retailer's messaging about marketing emails. These cases examine three different options: (1) an unticked box with a call-to-action to check the box to receive marketing messages; (2) a message to consumers that completing their transaction indicates their agreement to receive marketing messages subject to their unsubscribe actions; and (3) no message about marketing at all. Regardless of the messaging, the plaintiffs allege the retailers sent unlawful email marketing messages. While these cases focus on email at checkout, online checkout is likely not the only source of consumer emails at a company. Companies should understand how they collect emails at checkout and any other sources of email collection. It is possible that the same data point is collected via multiple means and by different teams across the business. Consider connecting with website teams, marketing teams, and agencies to better understand your company's practices and identify

potential risk.

Is the United States an opt-in to email marketing jurisdiction?

Not necessarily, but context matters. The federal CAN-SPAM Act continues to be an email “opt-out” or “unsubscribe” law. However, your email marketing program and guidance should factor in laws that regulate collection of personal information, including in specific applications like checkout. Other laws including state consumer privacy laws, the FTC Act, and state UDAP laws. The FTC Act and state UDAP laws prohibit unlawful and/or deceptive trade practices. These laws cover promises made by a company about how it will (or will not) use consumer data. For example, where a company gives a consumer an option to opt-in to email marketing the company should review any UDAP implications of sending a marketing email if a consumer’s option is ignored. As you learn about sources of email addresses you should identify if the source has any “rules” for using the email address. A “rule”, for example, that the source gave the consumer the option to receive marketing messages at sign-up (or not). A company can use processes and controls to manage eligibility of email sources for email marketing based on the consumer experience, unsubscribe status, etc.

Our discussion in this alert is focused on email collection under Massachusetts law, but online retailers should also be aware of cases in California challenging collection of IP addresses in online checkout experiences under the Song-Beverly Credit Card Act. You can read about that topic [here](#).

Copyright © 2025 Womble Bond Dickinson (US) LLP All Rights Reserved.

National Law Review, Volume XIV, Number 226

Source URL: <https://natlawreview.com/article/inbox-overload-massachusetts-lawsuits-target-online-retailers-email-collection>