

Beyond CAN-SPAM:

Understanding Preemption and the Scope of State Email Laws

Prepared by PossibleNOW's sister company, CompliancePoint

When organizations think about email compliance, they typically just think of the 2003 federal CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act, and not much else. That's because there's a widespread presumption that CAN-SPAM completely preempts state law in the world of email compliance.

If a federal law is preemptive, it means it overrides (or "preempts") any state email laws that impose contradictory or additional requirements. Notably, and by contrast, the Telephone Consumer Protection Act (TCPA) is not preemptive, which is why we see many state laws that are more restrictive than the TCPA.

CAN-SPAM's Preemption and Savings Clause (15 U.S.C. § 7707)

CAN-SPAM does indeed include a preemption clause, but it's not absolute. Here's what the law says:

"This chapter shall supersede any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, *except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.*"

In plain terms, this means that state laws that would purport to regulate commercial email generally are preempted. As a few examples, states would not be allowed to:

- shorten the CAN-SPAM 10-business-day timeframe for honoring opt-outs;
- mandate different formatting for unsubscribe links; or
- add additional disclosure requirements beyond CAN-SPAM's valid physical postal address requirement.

However, the italicized portion above (the "savings clause") means that **states are not preempted from enacting laws that target false, misleading ,or deceptive email statements or practices.**

Over the years, there have been around 20 states that have enacted laws addressing commercial email in some fashion, but only a handful remain that are likely not preempted by CAN-SPAM due to their focus on deception/fraud.

Around 15 or so have residual or dormant laws, most of which are preempted by CAN-SPAM, as many of them existed prior to CAN-SPAM's enactment.

Two notable states: Washington and California

Two of the most notable laws that target email deception and fraud—and that contain a private right of action—are **Washington's Commercial Electronic Mail Act (CEMA)** and **California's Business & Professions Code § 17529.5**. Both of these generally focus on false/misleading/deceptive headers and subject lines.

These laws highlight an essential point: even if businesses believe they'd never be the subject of CAN-SPAM enforcement from the FTC or state Attorneys General because of little to no enforcement, they can still be sued under one of these state laws — not because they impose additional requirements, but because they contain a private right of action which empowers private individuals to sue when emails are deceptive.

The Old Navy Case: Washington's CEMA in Action

A recent decision—**Brown v. Old Navy, LLC**—illustrates how these state laws work in practice. The plaintiffs in this case alleged that Old Navy sent promotional emails with subject lines like “Today Only” or “Final Hours,” even though the same sales continued well beyond the timeframes advertised. The claim? That these **subject lines created a false sense of urgency** and violated both CEMA and the Washington Consumer Protection Act (CPA).

Old Navy argued that CEMA's restrictions applied only when an email conceals its commercial nature, not when it exaggerates or misstates sale timelines. Initially, a federal court agreed. But on review, the Washington Supreme Court took a broader view. In a 5–4 decision, the Court held that CEMA “prohibits sending Washington residents commercial e-mails that contain any false or misleading information in the subject lines of such e-mails,” regardless of whether the deception relates to the commercial purpose.

The Court acknowledged concerns about liability for “banal hyperbole” but clarified that “mere puffery” (generally considered to be an exaggerated opinion rather than a fact that is measurable or provable) isn't actionable—only factual misrepresentations are. Under CEMA, **plaintiffs can recover \$500 in statutory damages per message**, making subject line accuracy a serious compliance concern.

California's § 17529.5

Washington isn't alone. California's Business & Professions Code § 17529.5 has also survived CAN-SPAM challenges. For example, in **Rosolowski v. Guthy-Renker**, the court allowed a private action to proceed under § 17529.5 where the plaintiff alleged **misleading subject lines and falsified header information**.

California courts have consistently held that this statute survives preemption because it targets deceptive conduct, not general email regulation. And like Washington's CEMA, § 17529.5 provides for statutory damages (\$1,000 per email) and a limited private right of action.

The Key Difference: Private Right of Action

CAN-SPAM can only be enforced by the FTC, state Attorneys General, and internet service providers. It does not include a private right of action for consumers.

That's where these state laws come in. The Washington and California laws—as well as states like Utah and Virginia—include private rights of action, allowing individuals to bring lawsuits against businesses for sending misleading or deceptive commercial emails.

Common Pitfalls: Misleading Subject Lines

Because of these state laws, businesses should be very careful in crafting their headers and subject lines.

A classic example: A business sends an email to a current customer with the subject line, “We’ve Been Trying to Reach You”. The consumer opens it, thinking there’s a billing or account issue, only to find a product promotion inside. That may be technically truthful (maybe you did try reaching out), but it can still be misleading. And if it creates a false sense of urgency or misrepresents the intent of the email, you could be vulnerable under state law.

The rule of thumb? All marketing copy—including subject lines and headers—should pass a two-prong test:

1. Is it truthful?
2. Is it non-misleading?

Statements can be truthful, yet be misleading if they omit key information, like the subject line example above.

Conclusion and Final Takeaways: Don’t Get Complacent

CAN-SPAM compliance is essential and should protect you from both federal and state claims if you truly meet its standards. But too often, marketers push the line with catchy, urgency-driven subject lines or ambiguous headers that walk the edge of being misleading.

Even if such messages do not get on the FTC’s or State Attorney General’s radar, it could give rise to a private lawsuit under state law — just like in the Old Navy case. Don’t assume low enforcement means low risk. Scrutinize your subject lines and headers the way a skeptical consumer (or plaintiff’s lawyer) might.

A few reminders for organizations and marketers:

1. **Don’t treat email compliance as an afterthought.** Minimal FTC enforcement doesn’t mean you’re off the hook—state laws are active, especially in states with plaintiff-friendly statutes, like Washington and California.
2. **Avoid factual misstatements in subject lines.** “Final Hours” means just that. If the sale is extended, you’re risking liability.
3. **Review your campaigns for state-specific risks.** Again, Washington and California in particular are high-risk jurisdictions for email litigation.
4. **Educate your marketing teams.** Even good-faith marketers often don’t realize that subject line wordsmithing can create legal exposure.

The lack of high-profile CAN-SPAM enforcement shouldn’t lull businesses into complacency, and email compliance should not continue to be a low-risk checkbox.