

Navigating Privacy Liability Coverage



A Guide for Insurance Brokers

Wrongful Collection is one of the fastest-growing exposures in cyber insurance. With new privacy laws emerging each year and an increasingly active plaintiff's bar, brokers need to distinguish comprehensive coverage from policies with critical gaps. Here's what to look for.

"Privacy Law" vs "Privacy Policy" Language

✓ LOOK FOR:

Insurance policies that define coverage triggers **based solely on violations of "privacy laws"** and do not include the requirement that the violation must also be pledged in the organization's "privacy policy."

WHY THIS MATTERS

While it is important for an organization to have a robust privacy policy, limiting coverage to situations where a violation of privacy law also constitutes a violation of the privacy policy can create coverage gaps.

Affirmative vs Silent Coverage

✓ LOOK FOR:

Insurance policies that provide clear, affirmative coverage for privacy liability outside of data breaches.

WHY THIS MATTERS

Cyber insurance policies typically cover traditional data breach litigation costs, but many are silent on wrongful collection and other emerging privacy claims. This ambiguity can leave policyholders exposed when newer types of privacy lawsuits arise, as ambiguous coverage may not be interpreted in their favor.

Avoid Language around "Unintentional Acts"

! WATCH OUT FOR:

Insurance policies that only cover **unintentional** privacy violations.

WHY THIS MATTERS

The line between "intentional" and "unintentional" is often unclear and can lead to coverage disputes. For instance, if marketing implements tracking pixels without legal review, is that intentional because they chose to do it, or unintentional because they didn't know it violated privacy laws? Policies that require proving an act was truly "unintentional" create ambiguity that may complicate claim disputes.

Common Exclusions to Avoid

! WATCH OUT FOR:

Because privacy liability is an emerging risk, some policies may exclude coverage for high-risk privacy exposures. Here are some specific exclusions to look out for:

- Wiretapping and unlawful surveillance
- Biometric Information Privacy Act (BIPA) violations*
- Tracking technologies and pixel use*
- Wrongful collection
- Facial recognition technology
- Voice recording and analysis

WHY THIS MATTERS

These exclusions target some of the fastest-growing areas of privacy litigation. If these exclusions exist, **look for endorsements or carve-back language** that restores coverage, especially for higher-risk industries.

**These exclusions are present in Coalition's Active Cyber Policy by default but may be removed via the Enhanced Privacy Liability Endorsement, subject to underwriting*

Coalition Coverage Overview

Looking for a cyber insurance policy that meets these standards?
Coalition's Active Cyber Policy¹ delivers.

✓ Coalition Active Cyber Policy

Comprehensive definition of Privacy Liability that includes:

- Violations of privacy laws regarding the collection, disclosure, sharing, selling, or use of PII
- Failure to comply with privacy policy provisions around data collection and sharing restrictions
- Breach notification law violations
- FCRA identity theft prevention and information disposal failures

⊕ Enhanced Privacy Liability Endorsement

This add-on endorsement expands protection by:

- **Removing BIPA exclusions** for comprehensive biometric coverage
- **Removing tracking pixel exclusions** for digital marketing protection

¹This product is only available on a non-admitted basis.

To learn more, reach out to your dedicated business development representative.