

WHITE PAPER

Non-Breach Privacy Risk: Is Your Business Covered?





Introduction

Cyber insurance has matured rapidly over the past decade, expanding from data breach coverage into first and third-party protections beyond traditional intrusions. As the regulatory and litigation landscape around data privacy has become increasingly aggressive, a gap in coverage has emerged that may not be fully realized until a class action lawsuit is filed, and insurance recovery is sought.

Unlike a traditional data breach, non-breach privacy risk (sometimes referred to as “wrongful collection”) does not require a hacker, ransomware attack, or any bad actor at all. It arises from a company’s own business decision to gather personal information, and it has become one of the fastest growing privacy risks in the United States.

Many policies stop short of providing clear, affirmative protection for non-breach privacy claims. As a result, companies may believe they have coverage, when, in reality, protection may be fully excluded or limited to defense costs only.

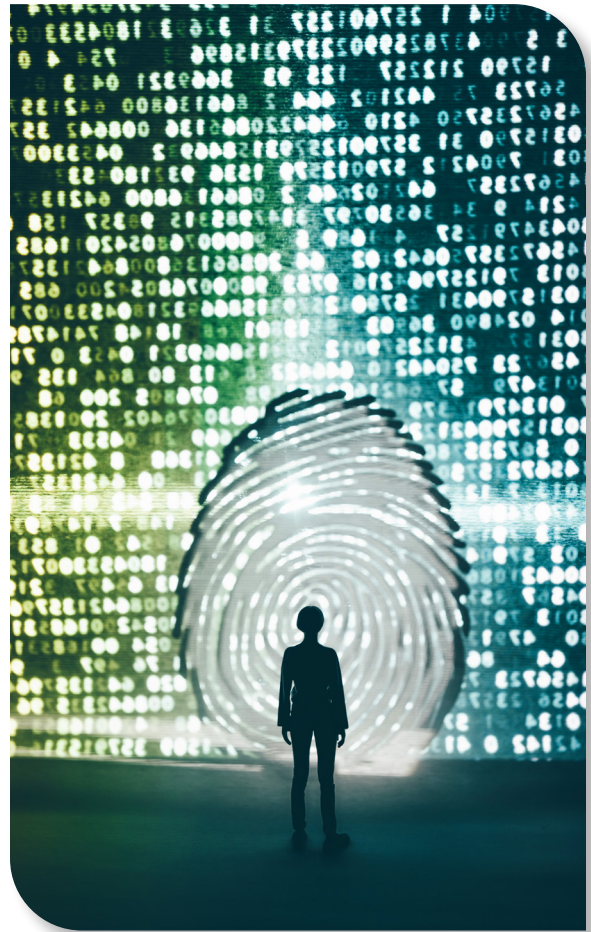
The growing prevalence of non-breach privacy litigation raises a critical question for insureds: **Does your company’s cyber policy provide affirmative coverage for non-breach privacy risks?**

What is Wrongful Collection?

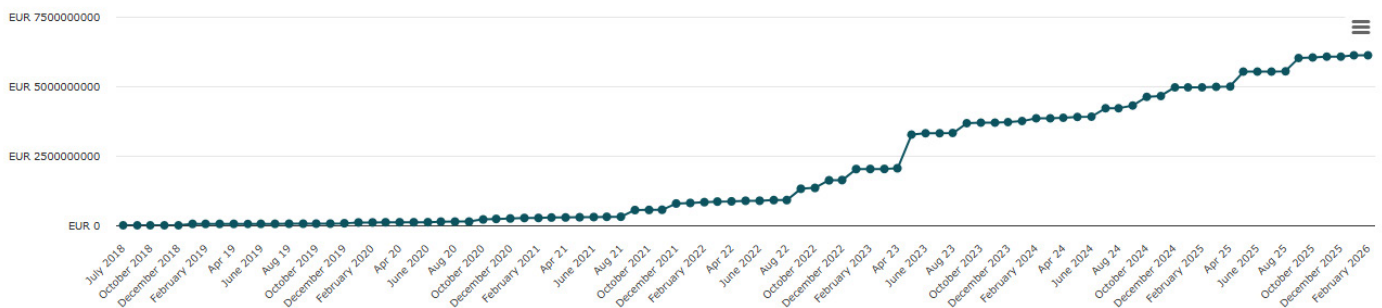
Wrongful collection is the unauthorized and unlawful collection or use of data that violates privacy laws, regulations, or user consent. Traditionally cyber insurance policies focus privacy coverage on costs associated with data breaches. However, with the rapid increase in the number of lawsuits and regulatory actions targeting how businesses collect and use data, the landscape is shifting. Wrongful collection is often used as an umbrella term, but it may be referenced by several different names within your cyber policy, including but not limited to:

- Non-Breach Privacy Liability
- Unlawful Collection
- Pixel/Software Tracking Technologies
- Wiretapping and Unlawful Surveillance
- Biometrics

The surge in wrongful collection claims over the past few years has been driven largely by plaintiffs' attorneys leveraging any number of privacy and wiretapping laws, including the California Invasion of Privacy Act (CIPA), Illinois Biometric Information Privacy Act (BIPA), General Data Protection Regulation (GDPR), Video Privacy Protection Act (VPPA), Telephone Consumer Protection Act (TCPA), and Electronic Communications Privacy Act (ECPA).



Total sum of fines



Note: The total sum of fines shown is specifically related to GDPR.

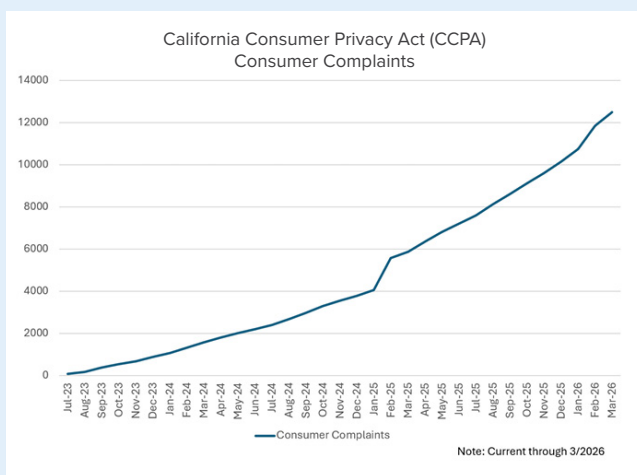
Source: CMS



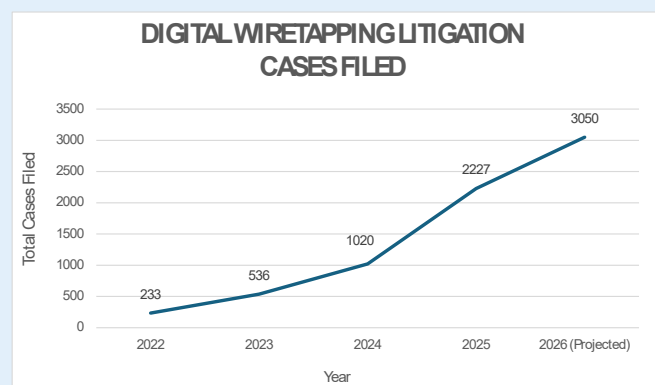
What can be covered?

Wrongful collection claims commonly arise from collecting or sharing personal data without proper notice or consent, including the use of tracking technologies (pixels, cookies, session-replay tools, chatbots, and analytics platforms), biometric data (fingerprints, facial recognition, retina scans, and voiceprints), location or device information (such as geolocation and identifiable IP addresses), and sensitive personal or health data. Claims are also frequently triggered by alleged inadequate privacy disclosures, invalid consent practices, or failures to disclose third-party data sharing.

It can be difficult to pin down the risk for such collection of information because the collecting often starts with the marketing group, who may or may not fully share such practices with legal and risk management. Further, it does not help that the legal boundaries are constantly shifting. Determining the appropriate measures to protect from non-breach privacy claims are challenging and need to be re-evaluated on a regular basis to align with the latest case law.



Source: [California Privacy Protection Agency](#)



Source: [Fisher Phillips, LLP](#)

Do you have full Affirmative Coverage?

Insurers offer a range of approaches to covering non-breach privacy risk. Coverage may be:

- 1 Fully excluded,
- 2 Sub-limited for defense costs only,
- 3 Allow defense costs up to the full policy limit,
- 4 Allow full affirmative coverage on a sub-limited basis, or
- 5 Provide full affirmative coverage up to the full policy limit.
- 6 Either full coverage for regulatory actions but limited coverage for civil suits, or vice versa

Brown & Brown recommends you ask your broker for what type of coverage your Cyber policy may (or may not) include.

Typical cyber policies generally exclude wrongful collection in their base policy language or by endorsement.

Defense costs are often included in wrongful collection coverage and are often the most heavily utilized benefit. Claims are commonly filed as class actions, and defense costs in class action litigation can run into the hundreds of thousands or millions of dollars before any indemnity payments are made.

Indemnity costs are frequently not covered. This can leave insureds on the hook for uninsured settlements and judgments due to privacy claims.

Non-breach privacy risk coverage remains a dynamic and evolving component of the cyber insurance market. As claim frequency and losses continue to increase, we expect insurers to shift underwriting strategies, adjust policy terms and conditions, and coverage parameters. Organizations will continue to face increased regulatory scrutiny, expanding privacy obligations, and growing claims activity. We encourage policyholders to remain vigilant in reviewing coverage structures and monitoring market developments to ensure their cyber insurance programs continue to address emerging non-breach privacy risks most effectively.



How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.



Find Your Solution at [BBrown.com](https://www.bbbrown.com)

Brown & Brown, Inc. and all its affiliates, do not provide legal, regulatory or tax guidance, or advice. If legal advice counsel or representation is needed, the services of a legal professional should be sought. The information in this document is intended to provide a general overview of the topics and services contained herein. Brown & Brown, Inc. and all its affiliates, make no representation or warranty as to the accuracy or completeness of the document and undertakes no obligation to update or revise the document based upon new information or future changes.

©2026 Brown & Brown. All rights reserved.