



Privacy Liability Claims Examples

Businesses of all sizes can experience cyber claims related to privacy liability and the costs associated with litigation or regulatory actions are often significant. The examples below illustrate how these claims can occur.



Digital Health Startup

VIOLATION TYPE: Pixel Tracking and Session Replay Technology

INDUSTRY: Healthtech

A prescription discount website operating in the US implemented tracking pixels and software development kits (SDKs) from multiple third-party vendors, including social media pixels and session replay technologies. These tools captured sensitive user interactions, including specific drug searches and pharmacy selections, without explicit consent.

Users discovered their medication searches were being used for targeted advertising across social media, and filed a class action lawsuit. They alleged that the platform's privacy policy failed to adequately disclose that health-related search data was being shared with third-party advertising platforms, which violated federal and state wiretapping statutes, consumer protection laws, and common law privacy rights.



Home Improvement Retailer

VIOLATION TYPE: Unauthorized Data Broker Sales

INDUSTRY: B2C E-commerce

A home improvement retailer shared customer purchase history, project preferences, and contact information with data brokers, who enriched the customer profiles with property records and income estimates. The enriched data was then resold to contractors, real estate investors, and financial services companies.

Customers discovered the practice when they received unsolicited contractor calls and aggressive refinancing offers. Plaintiffs alleged that the privacy policy's vague reference to sharing with "business partners for enhanced services" failed to disclose that customer data would be enriched and sold to unrelated third parties. The plaintiffs sought damages for invasion of privacy and disgorgement of profits from data sales.



Regional Restaurant Chain

VIOLATION TYPE: Third-Party Data Sharing
Beyond Stated Purpose

INDUSTRY: Hospitality/Food Service

A 20-location restaurant chain's online ordering system automatically shared customer data with delivery partners, including order history, contact information, and delivery addresses. While the restaurant chain's privacy policy mentioned sharing data for "order fulfillment," it failed to disclose that delivery partners used this information for their own marketing.

Customers discovered the unauthorized use when they began receiving promotional emails and targeted ads from delivery companies. A class action lawsuit alleges the restaurant violated state privacy laws by allowing unauthorized use of customer data beyond the stated purpose.



Orthopedic Clinic

VIOLATION TYPE: Health Data Pixel Tracking

INDUSTRY: Healthcare

A 150-employee orthopedic clinic installed Meta Pixel to track advertising effectiveness and build Facebook campaign audiences. The clinic's marketing team believed they had disabled automatic data collection for appointment pages, but "Automatic Advanced Matching" remained enabled.

The pixel captured form field data including patient names, searched conditions, and appointment types, transmitting this sensitive health information to Meta. Patients filed a class action lawsuit claiming HIPAA violations and unauthorized health data disclosure to Meta.



Online Tutoring Platform

VIOLATION TYPE: Undisclosed Data Sharing

INDUSTRY: Education Technology

An online tutoring platform shared children's detailed learning data — including academic performance struggles and behavioral observations — with educational research companies. The platform's privacy policy mentioned sharing with "educational partners" but failed to specify the commercial nature or extent of data sharing.

Parents discovered the practice when their children began receiving targeted ads based on platform activity. Parents expected "educational partners" to mean schools or nonprofits, not commercial entities. Plaintiffs sought statutory damages and the deletion of all shared data.



Beauty Retailer

VIOLATION TYPE: Missing Consent Controls

INDUSTRY: Retail/E-commerce

A beauty retailer's e-commerce website lacked proper consent banners and failed to recognize Global Privacy Control (GPC) signals, which are automated communications of users' opt-out preferences.

State regulators investigated the retailer after receiving consumer complaints about the missing opt-out mechanisms. The retailer agreed to a substantial settlement and was required to implement proper consent mechanisms, honor GPC signals, update service provider agreements with required privacy terms, and submit compliance reports to the state for two years.

The information above is designed to provide general information on the topic presented and is not intended to construe or render legal or other professional services of any kind. The litigation summaries above are primarily based on actual cases, however some information may have been altered, aggregated, combined, or anonymized. Coalition makes no assessment or judgment of the accuracy or validity of the allegations made. The reader is cautioned to consult independent professional advisers and formulate independent conclusions and opinions regarding the subject matter discussed herein. Coalition is not responsible for the accuracy or completeness of the contents herein and expressly disclaims any responsibility or liability based on any legal theory or in any form or amount, based upon, arising from or in connection with, for the reader's application of any of the contents herein to any analysis or other matter, nor do the contents herein guarantee and should not be construed to guarantee any particular results or outcome. Any action you take upon the information contained herein is strictly at your own risk. Coalition and its affiliates will not be liable for any losses and damages in connection with our use or reliance upon the information.