

4/24/2025



;Canadian Company Taking Data without Consent

SHOPIFY CANADA FACING CALIFORNIA DATA PRIVACY LAWSUIT

In a case very close to the GPR Collective Action, the case is being made that Shopify is the guilty party, in a class action.

While this may be true, GDP Complaint 1 reveals the scandal that it is the Browsers that is placing 'cookies' without consent. [@Shopify Canada Facing California Data Privacy Lawsuit ;-\)](#) la

A Case Highlighting the GPR Collective Action Campaign

A recent class action lawsuit against Shopify closely parallels the concerns raised by the GPR Collective Action Campaign, illustrating the widespread nature of privacy violations in digital commerce, under incompatible privacy regulation.

“Brandon Briskin, a California resident, alleges that Shopify installed tracking software—known as cookies—on his iPhone without his consent when he purchased athletic wear from the retailer I Am Becoming. According to the lawsuit, Shopify used his data to create a profile that could be sold to other merchants.” [Quoted from yahoo finance](#)

While Shopify bears responsibility in this case, Global Privacy Rights - Test Complaint #1 uses the

[ANCR Transparency Performance Indicator Report](#) (in public review) to reveal a more systemic issue: browsers themselves are placing 'cookies' without proper consent. The concept of "necessary cookies" has become a deceptive practice. As our campaign notes, even a child can recognize these are not baked treats, and privacy law clearly stipulates that permission is required to identify individuals and prior notice must be given before tracking users in the United States.

In our [Collective Action Complaint #2](#), we start from within the browser (surveillance tracking scheme) and uncover very similar violations in the healthcare sector. A medical walk-in clinic was found to have 17 trackers operating on its website, including Facebook pixels and keylogging software, directly violating Canadians' health privacy rights. Though the clinic

bears responsibility, it is also a victim of the broader web-browser ecosystem that enables companies like Shopify to collect data without proper consent.

The GPR Collective Action Campaign aims to address these systemic privacy violations by enforcing Transparency over identification, and require cookies to be upgraded to Consent Receipts, using the ISO/IEC 27560 Notice and Consent Record information structure. To both the direct perpetrators and those that use it like Shopify, for profit, enabling technological infrastructure accountable systemically.

Whats hidden even deeper is a fundamental difference in Privacy Regulation, in California, in a web browser people opt-out of surveillance, using a Global Privacy Control, which is a security control, as privacy has already been breached without consent, in a browser. For consent to operate online, an individual must “turn-on” identification tracking according to International Commons Treaty, implemented in EU by GDPR and in Quebec with Law 25.

Help us, test out new standards transparency tool for online surveillance and consent, sponsor this effort, [join the collective damages complaint](#), and going beyond California consumers (opt-in and out) protection, to make US online Surveillance something we need to turn on, to generate a consent receipt.

A strong Canada can create a digital environment where consent is meaningful and privacy rights are respected.

Global Privacy Rights