

Class Action Lawsuit Accuses Google of Violating Chrome Users' Privacy



A new class action lawsuit accuses [Google](#) of using its Chrome browser to record and send user information to Google regardless of whether the user syncs it or even has an account with Google.

Plaintiff Patrick Calhoun and others claim information such as IP addresses, cookie identifiers and browsing history are sent to Google without users' consent and against Google's promises that the information will not be sent.

The Google privacy class action lawsuit says the company has "unprecedented power to surveil the lives of more than half of the online country in real time" thanks to the presence of Google tracking code on websites "accounting for more than half of all internet traffic" and the fact that Chrome is the dominant browser used on desktop computers in the U.S.

The complaint also claims Google is misrepresenting its privacy practices because some of the company's third-party tracking cookies are "disguised" as first-party tracking cookies in order to "facilitate cookie syncing." The plaintiffs note the Federal Trade Commission has challenged these practices successfully in the past.

All versions of the Chrome Privacy Notice have promised the browser will not send personal information to Google unless a user decides to sync Chrome with their account, the complaint says.

Also at issue are x-client-data headers.



An x-client-data header is an identifier that can be combined with IP addresses and user-agents to identify each individual download version of Chrome.

The x-client-data identifier, which is sent from Chrome to Google every time users communicate online, was created and sent to Google with every communication since at least March 6, 2018, the Google privacy class action lawsuit alleges. The identifier has not been disclosed in any term of service or privacy policy.

Part of the problem with the alleged Google privacy breach is the fact that the company has a large network of affiliates, including Google Apps, Google Drive, Google AdWords and others, not to mention its business partnerships, the complaint states.

According to the plaintiffs, this means information that is shared with Google is fed "into a massive interconnected database of surveillance material."

“Google’s surveillance of the Plaintiffs and other Un-Synched Chrome Users directly contradicts its promises to honor users’ choice not to share data,” the class action lawsuit states. “This is a serious and irreversible invasion of privacy that is invisible to Google users.”

The plaintiffs say under California law, their personal information is a recognized form of property and has monetary value. So, in taking that personal information, Google is guilty of larceny and should disgorge any profits the company earned from that personal information, the complaint maintains.

The Google privacy class action lawsuit maintains that the motivation behind the breach was “to increase user engagement and increase revenue” for the company.

“Higher user engagement means more revenue in that moment for Google, and also more data about the users that can lead to more revenue,” the complaint says. “By promising more privacy, Google induces more private sharing, which is a more profitable kind of user engagement.”

The plaintiffs allege Google has violated the Electronic Communications Privacy Act, the Stored Communications Act, the Computer Fraud and Abuse Act, the California Unfair Competition Law, the California Computer Data Access and Fraud Act and the California Invasion of Privacy Act.

They also accuse Google of statutory larceny, invasion of privacy, breach of contract, breach of the implied covenant of good faith and fair dealing, intrusion upon seclusion and unjust enrichment.

The Google privacy class action lawsuit demands a jury trial and seeks an award of compensatory damages, including statutory damages, and interest; permanent restraint of Google from installing cookies that could track users’ “computer usage after logging out of Google or otherwise violating its policies with users”; court costs and expenses, including attorneys’ and experts’ fees; and any further relief deemed appropriate by the Court.

The plaintiffs seek to certify a Class including all Chrome users who opted to not sync their browsers and Google accounts while browsing the web between July 27, 2016, and present.

Did you opt out of syncing your Google account while using Chrome? Do you suspect your information has been sent to Google anyway? Tell us your thoughts in the comments.

The plaintiffs are represented by Lesley Weaver, Angelica M. Ornelas and Joshua D. Samra of Bleichmar Fonti & Auld LLP; Mitchell M. Breit, Jason ‘Jay’ Barnes, An Truong and Eric Johnson of Simmons Hanly Conroy LLC; Laurence D. King, Mario Choi, David A. Straite and Aaron L. Schwartz of Kaplan Fox & Kilsheimer LLP.

The **Google Privacy Class Action Lawsuit** is *Patrick Calhoun, et al. v. Google LLC*, Case No. 5:20-cv-05146, in the U.S. District Court for the Northern District of California, San Jose Division.