

RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:

COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

September 1, 2026

Sundar Pichai
Chief Executive Officer
Alphabet Inc. and Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Mark Zuckerberg
Chairman and Chief Executive Officer
Meta Platforms, Inc.
1 Hacker Way
Menlo Park, CA 94025

Shou Zi Chew
Chief Executive Officer
TikTok Inc.
5800 Bristol Parkway, Suite 100
Culver City, CA 90230

Dear Mr. Pichai, Mr. Zuckerberg, and Mr. Chew:

I write to urge Google, Meta, and TikTok to immediately change the default privacy settings for your ubiquitous tracking tools—Google Ads and Analytics, Meta Pixel, and TikTok Pixel—to protect Americans’ privacy and shield well-intentioned small businesses from massive, inadvertent legal liability.

Businesses pay Google, Meta, and TikTok to target specific audiences and measure the real-time success of their marketing campaigns. Millions of everyday small businesses rely on your platforms to survive and compete in the digital marketplace: they use Google Ads to reach potential customers and promote their products and services and Google Analytics to measure website traffic and page performance; they embed the Meta Pixel to deploy localized ads across Facebook and Instagram; and they install the TikTok Pixel to target advertising campaigns on TikTok. To make these paid ads effective, businesses embed your tracking scripts deep into their websites to capture exactly what pages consumers visit, what products they view, and what sensitive information they enter. This raw user data is funneled directly back into your proprietary algorithms to refine the behavioral profiles you maintain on hundreds of millions of Americans, rendering ordinary business owners the unwitting extraction agents for your advertising empires.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

2411 NW CARDEN AVE
SUITE 207
PENDLETON, OR 97801
(571) 364-6263

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

As state legislatures have stepped up to curb these invasive practices, your engineers have built features to disable specific privacy-invading practices. But these features, which are required for businesses to comply with various state laws, are disabled by default and can only be enabled by changing obscure configuration settings. For example, Google offers "Consent Mode" and regional "Restricted Data Processing" toggles to pause behavioral tracking and targeting. In addition, Meta and TikTok have developed "Limited Data Use" parameters that restrict data processing and halt custom audience targeting for residents in protected states—but only if a business manually alters its underlying website code or complex tracking configurations.

These compliance features are critical for businesses to comply with state laws like those in Oregon, where the Oregon Consumer Privacy Act (OCPA) grants consumers the right to opt out of targeted advertising and requires affirmative consent before processing sensitive data. Other states have enacted similar legal protections, including California, Colorado, Texas, Virginia, Connecticut, and Utah. Yet, instead of enabling the features that comply with state privacy law by default for customer websites using your tools, your companies bury these compliance features deep within complex developer menus and technical documentation, leaving them completely deactivated in standard installations.

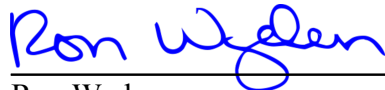
Compounding this failure is your platforms' refusal to natively and automatically honor Universal Opt-Out Mechanisms, most notably the Global Privacy Control (GPC). Under the laws of multiple states, including Oregon, California, and Colorado, businesses are legally required to recognize these browser-level privacy signals as valid consumer requests to opt out of data sharing and targeted advertising. Yet, instead of engineering your tracking scripts to automatically detect a GPC signal and immediately halt behavioral profiling out of the box, your companies require your business customers to manually implement complex custom code or deploy third-party consent management software to translate the signal and then trigger your opt-in privacy setting. By refusing to support GPC natively within standard installations, your platforms actively pass the engineering and compliance burden onto small businesses, leaving them legally exposed when standard configurations ignore a consumer's clear directive to stop tracking.

As behavioral economists and social scientists have long documented, defaults are powerful and most users and administrators never alter standard configurations. By making privacy-invasive tracking that is banned in several states the default, your platforms shift the entire burden of legal compliance onto small businesses, non-profits, and local organizations that lack the specialized legal teams or engineering resources to recognize their legal peril. When a local shop, a community healthcare provider, or a main-street business in Oregon deploys your tracking tools using your standard out-of-the-box configurations, they understandably expect that your tools allow them to comply with state or local laws out of the box – and do not expect that they are needlessly placed in severe legal jeopardy if they don't take further action.

Your platforms must transition to a strict privacy-by-default framework where your tools automatically restrict data collection in accordance with applicable state laws. I request that Google, Meta, and TikTok immediately update the default configurations for Google Ads and Analytics, the Meta Pixel, and the TikTok Pixel to strictly comply with state privacy laws out of the box and natively honor universal opt-out signals like the Global Privacy Control without requiring third-party software, ensuring that sensitive data is only collected after user consent where required. Please respond by September 29, 2026 with a plan to implement the changes requested in this letter.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian and Shreyas Gandlur in my office.

Sincerely,



Ron Wyden
United States Senator