



Google Chrome's Consumer-Oriented Solution for Handling Data Privacy

June 2019



When the Safari browser's Intelligent Tracking Prevention (ITP) protocol was announced, digital marketers rightly saw the move portending a major industry shift.

The “anything-goes” days of targeted advertising would give way to significantly more restrictive expectations for consumer data privacy. But even after Firefox followed suit, many brands still took a wait-and-see approach before committing to address the seemingly inevitable march towards a post-cookie world. That was because Google had yet to announce what its plans were for Chrome.

Chrome is the one browser that is dominant on both desktops and mobile. The day has finally come, however, and Google recently disclosed their plans. *[It remains to be seen if Google's timing and efforts are good enough to stave off what looks to be a tough regulatory environment for them to navigate in the near future as politicians on both sides of the aisle and industry watchdogs call for closer scrutiny of the company and other tech titans.]* Our take at PMG is that their move is the right one for the industry and, in fact, the most consumer-friendly of all taken by the major browsers.

A quick summary first, for those who missed what Google announced at its annual I/O developer conference. According to [MarketingDive](#):

- *New Chrome privacy settings will give consumers more control over how their browsing is tracked and shared with third-parties while maintaining first-party data.*
- *Developers will need to specify which cookies work across sites and which ones are for a single domain. This change will make it easier for users to block third-party tracking while retaining user preferences on a site.*
- *Chrome will also restrict fingerprinting, an increasingly common tactic adopted as a workaround when users have opted out of third-party tracking.*

These changes reflect a cascade of implications — from advertisers now being ever more reliant on first-party data, to their risky overreliance on walled gardens. They also reflect Google’s business model and the importance of demonstrable advertising effectiveness to the company’s financial goals. Google here shows its commitment to adding to the vitality and viability of the open web. This approach aligns the interests of publishers who make the content we love, consumers and users who read and watch content, and advertisers who want to connect with us in meaningful ways.

We at PMG think Google’s changes also represent a true step forward in how to address consumer data privacy issues. That’s because while Safari’s ITP approach essentially forced a specific solution for all users, Google’s changes will allow users to make their own choices. Consumers, based on their personal thresholds and preferences, will have the ability to opt out of how their data is used and shared for advertising tracking and targeting on Chrome.

[Whether or not they choose to opt out remains to be seen. Deloitte [research](#) showed that 31% of desktop users have ad blockers installed, and only 20% of Americans are using mobile ad blockers. And anyone who’s received their annual privacy notice from their banks and credit cards knows how likely inaction could be.]

The reality is that many consumers have brands they have loyalty or affinity for. They also have expectations that these brands understand and anticipate their needs, based on either products previously purchased or behavioral signals that convey their intent or interests. And that’s why PMG feels strongly that Google’s approach is the most consumer-friendly of all. Safari’s ITP says to these user segments that their preferences are insufficient and worth sacrificing in order to “protect” consumer data privacy en masse.

For advertisers, this will mean the environment in which they engage consumers will continue to change from the “old days.” They will find it very difficult, if not impossible, to serve personalized messaging to the super privacy-minded consumers. On the flip side, they could continue to have abundant insight and opportunity with the many consumers who don’t mind giving up their data in exchange for value and utility. And there will be a whole bunch of people in between those two ends of the spectrum.

However, that environment is changing already, because of ITP as well as regulation such as GDPR and the upcoming California Consumer Privacy Act. And news about the U.S. Department of Justice potentially developing an antitrust investigation into the company only adds to the general uncertainty. We at PMG and many marketers had already anticipated major changes. We knew that regardless of what Google decided to do, it was time to start prepping for the days when you could no longer rely on cookies for tracking and targeting at scale. If you haven’t already, we highly recommend checking out the [five key considerations](#) for marketers to prepare for the post-cookie future.

We will wrap this up by reiterating that the changes coming to Chrome are positive. These updates are positive for consumers because people should know how advertisers are using the data they’ve agreed to share, and they should have control on how to share it. The changes are positive for advertisers too. It will remind brands of their responsibility to ensure consumer interactions lead to a legitimate exchange of value. Otherwise, more and more consumers will rush to opt out without hesitation. ■

Digital Made for Humans™

Want to learn more about
people-based marketing?

Connect with us at insights@pmg.com

