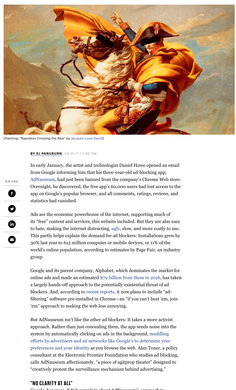
LONG READ

How Google Blocked A Guerrilla Fighter In The Ad War

The ad giant's eyebrow-raising decision to ban a Chrome app has been called the latest salvo in an unending, many-sided war over ads and privacy online.



[Painting: "Bayonet Crossing the Alps" by Jacques-Louis David]

BY ALI PABRAI.COM | ON 2.21.17 | 2:00 PM

SHARE

In early January, the artist and technologist Daniel Howe opened an email from Google informing him that his three-year-old ad blocking app, AdBlocker, had been banned from the company's Chrome Web store. Overnight, he discovered, the free app's 60,000 users had lost access to the app on Google's popular browser, and all comments, ratings, reviews, and statistics had vanished.

Ads are the economic powerhouse of the internet, supporting much of its "free" content and services, this website included. But they are also easy to hate, making the internet distracting, ugly, slow, and more costly to use. The gorilla blocking demand for ad blockers—Internet installations grew by 30% last year to 615 million computer or mobile devices, or 15% of the world's online population, according to estimates by Page Fair, an industry group.

Google and its parent company, Alphabet, which dominates the market for online ads and made an estimated $74 billion from them in 2016, has taken a largely hands-off approach to the potentially existential threat of ad blockers. And, according to recent reports, it now plans to include "ad-filtering" software pre-installed in Chrome—an "if you can't beat 'em, join 'em" approach to making the web less annoying.

But AdBlocksum isn't like the other ad blockers. It takes a more activist approach. Rather than just extending them, the app sends noise into the system by automatically clicking on ads in the background, muddling efforts by advertisers and ad networks like Google's to determine your preferences and your identity as you browse the web. Alan Toner, a policy consultant at the Electronic Frontier Foundation who studies ad blocking, calls AdBlocksum alternatively, "a piece of aggressive theater" designed to "creatively protest the surveillance mechanism behind advertising."

"NO CLARITY AT ALL"

Google, however, didn't complain about AdBlocksum's approach to protesting ads. Instead, it pointed to a developer agreement that gives the company "the right to suspend or ban any Product from the Web Store at its sole discretion," and offered a more prosaic reason for the ban:

> An extension should have a single purpose that is clear to users. Do not create an extension that requires users to accept bundles of unrelated functionality, such as an email notifier and a news headline aggregator.

Baffled, Howe wrote back to ask Google how this rule applied to AdBlocksum. In a second email, a company representative explained that an extension should not perform both *blocking* and *hiding* ads. In an email, a Google spokesperson confirmed to me that the company's "single purpose" policy was the reason for the app's suspension—but neither it nor AdBlocksum's developer could explain why AdBlocksum's clicks-all-the-ads approach made the threat of ad blockers by an order of magnitude.

"If there's considerable doubt over whether an ad click is legitimate or not, that's a big problem for Google charging for ad clicks," he wrote in an email. "It could undermine Google's business model more severely than pirate ad blockers, so it's probably their thought to 'nip it in the bud.'"

"The official reasons offered for their exclusion have been so generic as to provide no clarity at all," Toner said. "No exclusion needs an explanation."

ADS AREN'T JUST UGLY: THEY'RE INVASIVE

Google's decision to ban AdBlocksum was only the latest salvo in an ongoing war over online advertising. The industry and publishers have recently been fighting back against ad blockers, for instance, by requiring visitors to disable their ad blocks if they want to view a page. In August, Facebook announced it was blocking anti-ad software arrays in platform. And while AdBlocksum is the first desktop ad blocker Google has blocked, it has previously banned mobile apps like anti-tracking tool Disconnect and ad blocker AdBlock Fast from its Android Play Store, citing a rule that says one app can't interfere with another.

The ad industry also knows that ads can be a nuisance, and it's taking pre-emptive measures to make them more palatable—or, in Google's case, to block the unpalatable ones. "We feel like there are a lot of challenges in advertising. There are a lot of wrong ways," Doris Fitzhart, vice president of Chrome engineering, told Ohio last year. But "if publishers and advertisers do ads the right way, it can be great for them and for the ecosystem."

But Google's positions also point to a crucial disagreement at the heart of the ad war: What makes ads such a nuisance to begin with?

Advocates insist that ads aren't just ugly, annoying, and bandwidth-sucking. They pose a risk to privacy, as the networks of software behind ads—cookies, trackers, and malware—work not only where you go on the web but, through tracking phone and your purchases, what you do in real life. This data, which helps data brokers better understand you, includes everything from your sexual life to your shopping and financial habits to your political and religious views.

But privacy is largely missing from Google's discussion of problematic ads, says Howe. By simply mentioning AdBlocksum's actual intent, Google's explanation for banning it echoes the advertising industry's discussion of web ads, which focuses on aesthetics rather than privacy.

"Google does not want the ad-blocking debate to be about surveillance and civil liberties because it lays weak arguments to make them," he wrote in a post on the blog of Princeton's Center for Information Technology Policy. Instead, "it would like to keep the debate to the economics and aesthetics of ads."

Mobile ad blocker use—much of it in Asia—now outpaces use on desktop browsers. [Chart: PageFair]

With a built-in ad filter for Chrome, which commands an estimated 60% of the browser market, Google could continue to frame the debate in terms of aesthetics rather than in terms of privacy.

Google's ad filter would be based on standards drawn up last month by The Coalition For Better Ads, a global coalition of advertisers cofounded by Google and including industry groups, publishers like Facebook and The Washington Post, and advertisers like Proctor & Gamble and Unilever. Apple, which permits third-party ad blockers on its Safari browser on iOS Mozilla, which includes anti-ad features in its Firefox browser, are not part of the Coalition. The new guidelines aspire to change the ecosystem of the industry to stop using the kind of annoying ad formats that have fuelled the rapid rise of ad blockers, like pop-ups, auto-play video ads, and full-screen ads. But the standards do not mention tracking or user privacy.

"By banning AdBlocksum and then rolling out its own ad blocker, Google is now trying to prevent anyone else from drawing the line in the sand where it comes to which ads are presented to the user," Zer-Aviv said. Google would be "leveraging its near monopoly in the ad blocker/adware markets to forcefully exclude any competition that does not align with its model of 'acceptable ads,' be it other ad networks, the No Dot Track standard, or privacy initiatives like our own."

Google's advertising business depends upon tracking more than ever. A little-noticed change to the company's privacy policy last year gave it the ability to track users' web activity across a majority of sites and apps. On a concession to privacy, the company also allows users to change their default settings to "opt-out of ad personalization."

Google's ad blocker could give the company more leverage over advertisers and other ad blockers that have recently launched so-called "Acceptable Ads" programs, which permit some ads to be shown that are deemed to be "non-intrusive." Google and other major ad networks already pay to participate in AdBlock Plus's acceptable ads program, which provides the bulk of revenues for Eyeo GmbH, the company that makes the app.

A Google ad filter could also effectively suppress a new Do Not Track standard. The older standard is essentially an automated request from your browser, asking the websites you visit to refrain from tracking you. The new version of DNT, developed by the Electronic Frontier Foundation, is dynamic: It asks websites not to track you and it knows if they comply.

In its most recent update, AdBlocksum permitted sites that complied with the Do Not Track policy to display ads to users, and refrained from clicking on those ads. (Because Google does not comply with DNT, the app blocked Google resources such as DoubleClick.net and Google Analytics.)

Howe thinks the new DNT feature may have contributed to Google's decision to ban AdBlocksum from the web store.

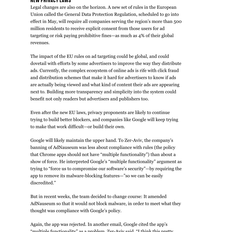
The standard may be threatening to Google. Howe wrote in his blog post, "perhaps because it could represent a real means for users, advertisers, and content providers to move away from surveillance-based advertising." If enough sites adopt the Not Track, "there will be significant financial incentive for advertisers to place ads on those sites, and those ads will be bound by DNT, as the mechanism also applies to a site's third-party partners. And this could possibly set off a chain reaction of adoption that would leave Google, which has committed to surveillance as its core business model, out in the cold."

Toner, of the EFF, said "it does seem like a strange coincidence" that AdBlocksum was banned soon after it integrated support for the new DNT standard. Perhaps, he said, the EFF's own Chrome app that blocks cross-site trackers, also supports the new DNT standard, but it has not encountered problems with Google, he said.

Cable companies are also seeking a piece of the marketing pie on which Google, Facebook, and other digital media giants are already hunting. The bill President Trump signed last month to repeal privacy rules for internet service providers will allow these companies to collect and sell customers' browsing data to third parties without their express consent.

The playing field is growing ever more sophisticated too, as companies combine web data mining with personality behaviors gleaned via Facebook to better profile consumers and target them with ever more persuasive ads, be it for pay-gates or politicians. "We think that ISPs should not be helping track their users," said Cooper Quintin, a security researcher and programmer at EFF.

Nor do most Americans, according to a survey by YouGov and the *Huffington Post*. Seventy-one percent of the public—and 71% of Republicans—believe the FCC's privacy rules should have gone into effect (see the interactive chart below). Some states, meanwhile, including Minnesota and Washington, are contemplating new privacy rules to pick up the slack.



Users who want privacy from ad tracking can use a variety of free and subscription-based software to defend themselves. Tower suggests installing tools like Privacy Badger, Disconnect and uBlock, beefing up ad-blocker settings in the Easyprivacy filter, and turning off Acceptable Ads in AdBlock Plus or AdBlock for Chrome. Browsers like Firefox, Epic, or Brave also include ad blocking and anti-tracking features.

Meanwhile, new technologies for ad blocking, including a prototype "perceptual" ad blocker developed by researchers at Princeton and Stanford, promise even more effective ad blocking in the future. And Google, Facebook, and other tech rivals in Firefox and Opera, while enterprising Chrome users can manually install the app in developer mode.

NEW PRIVACY LAWS

Legal changes are also on the horizon. A new set of rules in the European Union called the General Data Protection Regulation, scheduled to go into effect in May, will require all companies serving the region's more than 500 million residents to receive explicit consent from those users for ad targeting or risk paying prohibitive fines—as much as 4% of their global revenues.

The impact of the EU rules on ad targeting could be global, and could dovetail with efforts by some advertisers to improve the way they distribute ads. Currently, the complex ecosystem of online ads is rife with click fraud and distribution schemes that make it hard for advertisers to know if ads are actually being viewed and what kind of content their ads are appearing next to. Building more transparency and simplicity into the system could benefit not only readers but advertisers and publishers too.

Even after the new EU laws, privacy proponents are likely to continue trying to build better blockers, and companies like Google will keep trying to make them difficult—or build their own.

Google will likely maintain the upper hand. To Zer-Aviv, the company's banning of AdBlocksum was less about compliance with rules like policy that Chrome apps should not have "multiple functionality"—but about a desire of Eaves. He interpreted Google's "multiple functionality" argument as trying to "force us to compromise our software's security"—by requiring the app to remove its malware-blocking features—"so we can be easily discredited."

But in recent weeks, the tracker decided to change course: It amended AdBlocksum so that it would not block malware, in order to meet what they thought was compliance with Google's policy.

Again, the app was rejected. In another email, Google cited the app's "multiple functionality" as a problem, Zer-Aviv said. "I think this pretty much seals the question about Google's sincerity on the reasons for the ban against AdBlocksum."

As he and his cofounders argue, real progress in online privacy isn't about the option to see less annoying ads. It would require corporate policy and government regulations to align to give users an option to fully opt out of online tracking if they want to. Until that happens, anything less isn't much of an option at all.

With additional reporting by Ali Pabrai.com.

ABOUT THE AUTHOR
Ali Pabrai.com is a writer with bylines at Inc, Motherboard, Creative Scripts & Confused and The Guardian. He's also a photographer, psychogeographer and Pomeranian. More