Jan 20 2020

Privacy Browsers Advertising

Brief #20: Google Chrome & the reinvigoration of browsers around privacy

14 min read

What's Happening

Recent months have seen renewed energy in the browser space, shaking up an arena that has had a relatively stable leaderboard. **Google's Chrome has been the confirmed leader** with 64% market share, Apple's Safari the clear #2 with 18% share, and the rest a long tail that includes Mozilla's Firefox, Microsoft's Internet Explorer and Edge, and smaller players such as Brave and Vivaldi. However, **with the rise of privacy and security as consumer issues, and Google the only browser player with a big ad business, Chrome's position has become increasingly vulnerable**.

In response to a spate of privacy-oriented moves by competitor browsers (see below), leading browser **Chrome came out with the news on Jan 14 2020 that it planned to phase out 3rd-party cookies within two years**. The news sent the share prices of some adtech companies crashing. 3rd-party cookies are set via a code snippet on a website and used by third parties (such as advertising, analytics, social-plugins, and live-chat services) to follow users across the web and gather browsing data. **One common use is to retarget consumers with ads placed on other sites visited**. In contrast, 1st-party cookies are collected by the website the user is on and typically used to support a consistent and efficient experience (e.g. language preferences, shopping carts, staying logged in). Google can track users of its own products, for instance, as 1st-party data.

Google continues to be supportive of "an ad-supported web." The two-year timeline was intended by Google to allow for open-standard alternatives to emerge – such as its Privacy Sandbox – that **facilitate personalization while maintaining privacy**. The move, however, is raising alarm from marketers and ad agencies, and will likely have sweeping implications for publishers, data-management platforms, and adtech firms as well.

The browser is the latest front in the war for direct relationships with consumers, with privacy becoming table stakes for browser players.

» Jump to **What It Means**

Key trends involved

- **Browser as a consumer-facing quasi-"operating system"**: On average, 60% of time spent on the PC is in a browser. Browser players have been working to up engagement through **applications/extensions and integrations**:
  - **Microsoft**'s decision to build the new well-reviewed Edge on Chromium (Google's open-source browser project; see below) means **access and integration with Chrome extensions**, piggybacking on Chrome's developer ecosystem and offering a familiar experience. Microsoft also announced in Dec 2019 the Edge Addons Store, which already has hundreds of applications. It's also building in integrations between Edge and Office suite, such as Collections that help users gather and export internet research to Word or Excel.
  - **Google**, in turn, has reaffirmed support for Chrome browser extensions, while shutting down packaged apps for Chrome OS (which runs on Chromebooks). In Nov 2019, it launched **Google Duplex as "Google Assistant in Chrome"** to help Chrome users complete tasks such as buying movie tickets. Google also has been **using the "new tab" interface on the Chrome mobile browser to present personalized news** – offering a more engaging experience and becoming a major driver of traffic to news sites.
  - **Apple** also added **Siri Suggestions and stories from Apple News** to the Safari mobile start page, under the latest release in Sep 2019.
  - **Vivaldi**, a smaller player, is offering a **highly customizable experience for advanced users**, and, as a Chromium-based browser, also has access to the Chrome extensions library.
- **Privacy as a major competitive dimension**: Recent moves across the browser landscape (see below) are underscoring the emergence of privacy as a prominent dimension in the browser wars. **Chrome is not the first player to block 3rd-party cookies – it was preceded by Safari and Firefox**, which are both angling for position as privacy-focused

leaders. Smaller privacy-oriented browser **Brave** is also gaining traction with 10M monthly active users as of Dec 2019, doubling over the past year. **Microsoft**'s moves have been particularly notable, with **privacy features in the new Edge browser built on Chromium**.

- **Browsers on the front lines of cyber attacks and security**: Even Firefox, which has a reputation of being among the more secure browsers, was recently subject to targeted attacks when a "zero-day" vulnerability was exposed. **Browser-based code attacks** – malicious code injected into the 3rd-party scripts common in modern websites – are increasingly common as well, prompting a rise in vendors with solutions (e.g. Cloudflare for Teams). **Extensions** are another source of trouble – even extensions from established firms like Avast/AVG can be a source of unwarranted data-harvesting. Tech firms are even policing national governments, with Google, Apple and Mozilla recently blocking an untrusted certificate issued by Kazakhstan that was used to monitor its citizens' internet traffic.

- **Encrypted website requests are placing limits on monitoring and controls**: DNS-over-HTTPS (DoH) is a security protocol that encrypts DNS (Domain Name System) requests, which look up the IP address from the website domain when a user needs to go to a website. For a long time, DNS requests were executed openly through plain-text transmissions. This made it possible for third parties to track browsing and left such requests open to malicious actors (e.g. routing a user to fake versions of the site). DoH uses secure HTTPS (Hypertext Transfer Protocol Secure) communication to **limit third parties like internet service providers (ISPs) and cybersecurity agencies/firms from monitoring the websites users visit**. Microsoft announced in Nov 2019 that Windows 10 would adopt DoH, joining Mozilla Firefox (Sep 2019), Google Chrome (Sep 2019), and Opera (Oct 2019). Other browsers built on Google's open-source Chromium project, such as Microsoft Edge, Brave and Vivaldi, will also have the ability for DoH to be turned on. DoH is controversial, with critics saying that DoH still leaves gaping security holes and **bypasses enterprise controls and national blocklists**.

- **Privacy regulation:** The California Consumer Privacy Act (see our Dec 30 2019 brief), which just went into effect, requires that certain companies "doing business" in California comply with rules governing how they collect, manage, and use personal data, both online and offline. Some companies, including Microsoft, have committed to **applying CCPA rules to all customers nationally**. The CCPA's **requirements to notify consumers at data collection and to stop selling an individual's information upon request** will impact how consumer data (e.g. from cookies) is gathered and used. The CCPA is very popular among California voters – nearly 90% are in favor. **Tech firms are lobbying for federal privacy regulation**, seeking a more consistent and coherent regulatory framework rather than a patchwork of state-level laws.

- **Personalization with privacy: Google** has been working for nearly 5 years on ways to protect user privacy under the advertising business model, going back to Chrome's **differential privacy techniques that can describe patterns of groups while withholding individuals' information**. Around 2017, Google built a double-blind encryption technology that allowed it to anonymously match users viewing online ads to

purchases in brick-and-mortar stores, using Mastercard data. In Aug 2019, Google launched its Privacy Sandbox to experiment with mechanisms that enable personalization while protecting user privacy – e.g. anonymous aggregation of user data joined with "federated machine learning." Some publishers like Meredith and Washington Post are working on forms of **contextual advertising** that are less reliant on cookies (e.g. that use the content the user is viewing on the page or the channel the visitor came from). The dynamic extends to search engines as well, with Verizon's new privacy-focused OneSearch offering only contextual ads based on search terms entered.

Moves by other browsers in privacy

- Apple's **Safari**, which is deeply integrated with iOS and iCloud, has long emphasized user privacy and protecting users within its ecosystem. It initially **blocked 3rd-party cookies by default in 2017 under a feature called Intelligent Tracking Prevention (ITP), the first major browser to do so**. It followed with several updated releases in 2019, addressing technical loopholes that had allowed third parties to continue tracking users across domains. It also added a feature limiting publishers' ability to detect a user in private browsing, reducing their ability to meter content. In Nov 2019, Apple published a series of whitepapers detailing current and planned privacy features in Safari, photos, and location services, and launched a redesigned privacy page highlighting its stance that "privacy is a fundamental human right." Apple's emphasis on privacy has impacted publishers, which report **30% to 60% less value (in cost per thousand impressions) from their ad inventory** through Safari (vs. Chrome).
- **Firefox**, housed under a corporation owned by the nonprofit Mozilla, has also been making a strong play for the privacy-focused user over the past few years. It recently announced it will **allow users to delete their collected data**, following an array of new privacy features released in 2018 and 2019. In Mar 2018, it launched a Facebook Container feature **preventing Facebook from tracking user activity across the web after they leave the site**. Firefox then in Oct 2018 launched "**Enhanced Tracking Protection**," giving users the ability to block 3rd-party cookies before making it the default in Jun 2019. In Oct 2019, Firefox added a Privacy Protections dashboard for users showing the trackers it blocked. **Firefox has faced financial challenges of late – it laid off 70 employees to preserve funding** to expand into areas such as password management, file-sharing, and private VPN connections.
- Microsoft's new **Edge** browser, built on Google's open-source Chromium project, was just deployed this month as an automatic Windows Update to Windows 10 computers. Edge is **available for both Windows and MacOS, and aims to hit 1B users**. Being built on Chromium means the Edge experience is as fast and functional as Chrome with similar website compatibility. Edge can also readily transfer settings and bookmarks from Chrome and access Chrome extensions. With that, Microsoft is **focused on competing in new areas such as Office integrations (e.g. Collections), Edge-only extensions, and privacy features**. Edge offers an InPrivate browsing mode that does more to dissociate

users from their activity (some "private browsing" modes in other browsers don't fully anonymize user activity from parties like employers). Edge also has a more advanced **Tracking Prevention** feature that blocks websites from tracking user activity, which will be on in the default "Balanced" security mode. Microsoft plans to roll out 2-3 new major features for Edge every year and has **signaled the end for Internet Explorer** (which has the highest proportion of users enabling 3rd-party cookies).

- **Brave**, a privacy-focused browser also built on Chromium, officially launched out of beta in Nov 2019. Available on Windows, macOS, Linux, Android and iOS, Brave has 10M+ monthly active users and growing. Features include blocking of ads, tracking and autoplay by default. It also offers **two private modes, with and without use of Tor** (an open-source software project for anonymous communication). Where Brave breaks ground is in its **cryptocurrency-based Brave Ads / Brave Rewards program**. Users are paid to browse and watch ads, with 70% of ad dollars going to the user and 30% to Brave. Users can withdraw their Brave Rewards tokens or use them to "tip" content creators. 30K publishers have opted into the Brave Rewards platform, including small individual influencers and brands like The Washington Post and The Guardian.
- Other notable browsers and recent enhancements include: **Opera**, which released a tracking blocker and free unlimited VPN in Oct 2019; and Chromium-based **Samsung Internet**, which launched in Oct 2019 with an enhanced Secret Mode that includes password protection and anti-tracking. **Tor**, meanwhile, is known as one of the most secure browsers, built specifically for anonymity and circumventing tracking and censorship. Alibaba-owned **UC Browser** (the 5th-most popular browser by market share globally) has, notably, accumulated a reputation for being short on privacy features.

What It Means

The story around browsers by itself might seem a bit esoteric and technical in nature. We should view it, however, as **a critical front in the broader sweeping transition towards direct relationships with consumers**. It's a transition with the potential to break the business models of adtech firms (particularly those focused on retargeting), ad agencies, retail and consumer brands, data brokers, credit agencies, financial services companies, telecom companies, and beyond.

Let's take a step back and consider from the consumer vantage point how they engage with technology. On a mobile device, there are a series of "windows" to the customer – the mobile device, the mobile operating system, the mobile app or browser, and the in-app experience or website. First, there are relatively few major players in mobile devices (Samsung, Huawei, Apple) and mobile operating systems (Android, iOS). Second, the more intimate knowledge of

the user comes from the deeper layers closer to the points of interaction. **The browser is a key channel with visibility into a broader array of user behaviors and interests**. In its role as gatekeeper near the user's intent or need, it is more akin to a search engine, ecommerce platform or "super app" (see our Dec 13 2019 brief).

For the big tech firms, the browser represents another channel for winning a share of users' time and attention. **The more users interact with their browser, the more opportunities to entangle them in their ecosystem and drive them to other services**. For instance, Chrome is "exceptionally profitable" for Google if you consider the lifetime value of a Chrome user. With each new Chrome user, Google saves on the "search royalty" it pays to other browsers for making Google the default search engine. It also locks in users of Google, enabling conversion to integrated Google services like Gmail and Drive as well as collecting swaths of data that can be used to develop personalized user profiles for its advertising business. With **the ongoing evolution of browsers into a quasi-OS with integrations and app-like experiences**, we will likely see users spending more of their time within them. Winning in the browser wars could mean a significant moving of the needle in bringing consumers into the funnel toward other digital products.

The browser also represents an **opportunity for big tech firms comparable to an AI voice assistant – the ability to insert themselves as a trusted channel or even advisor**. Leading browser players such as Google and Apple want to position themselves as the personalized AI–powered interface between the user and the universe of information, services and products they might need. This role will only rise in prominence as privacy regulation (see our Dec 30 2019 brief) makes it harder to sell/share data and target users.

Trusted companies with access to first-party data will work to own and act on more of the data they collect, rather than pass or sell to outside parties. Google, for instance, has access to an enormous amount of 1st-party data from its own search engine and applications, as well as from running code on many websites and apps. As we have said before (see our Jan 10 2020 brief on the gig economy), trust is the universal lubricant that reduces friction and streamlines exchange. For the big tech firms – even for Google with its ad business – the shift away from 3rd-party cookies has the **potential to solidify their dominance**, assuming they can position themselves among the trusted brands.

On the other hand, **consumers are becoming less tolerant of data practices – even those formerly acceptable – that lack transparency and consent**. Firefox, for instance, pointedly highlighted in a Nov 2019 letter to Congress the **privacy and security practices of internet service providers** (ISPs). Examples include their sale of location data to other parties without user consent, manipulation of DNS to inject ads, Verizon's tracking of sites visited by 100M users through "super-cookies" that can't be deleted, and AT&T charging users $29/month to opt out of sale of their browser history for targeted ads. **We can expect both consumers and lawmakers to be unsympathetic to ISPs as they lose access to consumer data** (e.g. due to encrypted website requests).

Among the browser players, Google is still operating from a position of power. With a dominant lead in the browser market, it would take a prolonged and egregious strategic oversight to topple Chrome from the top position. While Chrome has lagged in privacy compared to other browsers Google has the technical prowess and market weight to move the industry as it makes deliberate moves with an eye on its advertising business. Its recent announcement, along with initiatives such as the Privacy Sandbox, signal Google's commitment to bringing a technical solution to life that can balance user privacy and an advertising-based business model. **More likely than not, Google wouldn't have made the public announcement if it weren't confident that it was technically viable**.

That said, **Chrome faces some serious contenders** in Microsoft's new Edge browser and Safari, not to mention a host of other players built on Google's Chromium open-source project with all of its attendant advantages (e.g. speed, compatibility across websites, portability of settings, access to Chrome extensions). Many of Chrome's differentiators are now table stakes. With competing browsers now having to innovate above and beyond, we can expect to see **more investment in extensions and "add-on" stores, integrations within their own ecosystem and with partners, avenues to 1st-party data, and AI-powered in-browser experiences**.

Browsers from outside big tech – e.g. Firefox, Opera, Brave – will play **niche roles serving user needs distinct from the mainstream**. We'll see them bring more novel business models, such as Brave's cryptocurrency-based rewards program. **However, they lack the key advantages of technical scale and hardware/operating system-based reach**. They'll find it challenging to match the investment of the big tech firms. Furthermore, if they do come up with a new feature, it could be vulnerable to a fast-follower copycat response from the tech firms. They also lack the ready audience that Chrome enjoys in users of many Android devices and Chrome notebooks, that Edge has in users of Windows devices, and Safari in users of Apple devices.

The announcement that browser leader Chrome will phase out 3rd-party cookies is a **body blow to the advertising industry**. A significant portion of digital ad-buying today depends on the targeting afforded by 3rd-party cookies. When Firefox blocked 3rd-party cookies, website publishers in Germany (where Firefox has greater market share) saw a 38% decline in bid rate, 45% decline in revenue, and 23% decline in cost per thousand impressions. According to Google's own study, less-relevant advertising without cookies results in **52% less funding for publishers**.

For some business models – e.g. third-party data and data management platforms, vendors providing "multi-touch attribution" of credit through the marketing funnel, associating user impressions to installs ("view-through attribution") – **there is no alternative to 3rd-party cookies today**. Past efforts to block 3rd-party tracking by browser players had previously left loopholes that meant those business models were still viable. Now, browser players are actively **working to close these loopholes** (e.g. Google's work to restrict "fingerprinting" of

browsers using information such as fonts installed and device type, Safari's series of Intelligent Tracking Protection releases).

Given prior moves from Safari and Firefox to block 3rd-party cookies, the response from the **advertising industry has been disappointed rather than surprised**. Instead of seeking a wholesale pullback, they are making a bid for more time and confirmation that alternatives would be available, saying: "It may choke off the economic oxygen from advertising that startups and emerging companies need to survive." Across industries, those that rely on third-party data (e.g. automakers) will be impacted more than those who own first-party data (e.g. direct-to-consumer brands).

The next two years will go by quickly as tech vendors and industry players work on solutions. With Google heading towards open standards, we may see the emergence of **"privacy-safe solutions" that work across all browsers and apps**. Current proposals include a "browser sandbox" that collects clicks and conversions, metering out data strictly and controlling the user's privacy. Another proposal suggests that the browser sandbox could do match ad clicks to conversions, reporting back to the advertiser only in a batch.

As advertisers and publishers look towards a "post-cookie world" (or at least one without 3rd-party cookies), we can expect **more investment in differential privacy and federated machine learning** (using patterns of groups rather than individual data), **contextual advertising** (which serves up ads based on non-personal data such as the content of the page), **consent mechanisms** (e.g. requests to register and sign in), **advertising inside walled gardens** (using 1st-party data), and "**data clean rooms**" (where 1st-party data from multiple entities can be pooled and users matched without being identified).

The "media mix" will shift towards marketing creative that can generate clicks or other direct response, or can bring consumers into a 1st-party environment. Advertisers will also return to brand awareness campaigns again. We'll see **big publishers – who are recognizing the value of their 1st-party data – develop their own ad platforms** (e.g. Walmart, NBCUniversal, Vox) **and grow their walled gardens**. There will also be more emphasis on advertising on other consumer touchpoints that are growing – e.g. connected TV, podcasting (see our Dec 3 2019 brief). A few large trusted vendors will emerge to serve key roles – such as gatekeepers of "data clean rooms" or new user-ID solutions.

Players will still have to be wary, however, of seemingly non-personal contextual data. In the UK, the data-sharing involved in real-time bidding on ad inventory is being reviewed by regulatory authorities under the EU's GDPR (General Data Protection Regulation). Google announced in Nov 2019 it would remove contextual content information from bid data sent to ad bidders, while continuing to include more personal data like user location and unique device ID. The move, according to industry observers, was to appease the UK's Information Commissioner's Office (ICO) and designed to prevent adtech companies from "listening in" to auctions to build consumer profiles.

Disclosure: Contributors have investment interests in Microsoft. Google is a vendor of 6Pages.

Have a comment about this brief or a topic you'd like to see us cover? Send us a note at tips@6pages.com.