

The Use of Online Trackers Across Various Websites

Abrahm Hill

I. The Nuts and Bolts of Online Tracking

The issue of online behavioral tracking of internet users while accessing websites and apps has seen a steady rise over the past two decades. Websites and apps employ two primary methods for gathering information on users: first-party tracking and third-party tracking.¹ First-party tracking allows a company to collect data on a user visiting its website.² For instance, Google may gather information on a user's search queries, location data, and contact information. In contrast, third-party tracking allows companies to collect data on users while they are on different websites.³ For example, a person browsing for luxury goods on Facebook may be tracked by marketers outside of Facebook (e.g., Versace or Gucci), who then send the user targeted luxury clothing ads.

Various online tracking technologies are employed to collect data on consumer activities.⁴ Websites often utilize cookies, which are data pieces stored on a user's device, uniquely identifying them.⁵ These cookies can only be read by the marketing company that sent them, whether it is a first-party or a third-party.⁶ Pixels are also used to track user actions and transmit information.⁷ Pixels are small images or bits of code that send details about a user's actions to the pixel's owner.⁸ Additionally, digital fingerprinting is used to track user activities, exploiting unique aspects of each computer's behavior to identify the user.⁹ A more invasive tactic is keylogging, which records a user's typing in a text field.¹⁰ Perhaps worst of all, a website may use session recording, creating a real-time video recording of everything a user does on a website – every click, mouse movement, and word typed.¹¹

II. The Blacklight Test

To assess the prevalence of online tracking, I used a tool known as “[Blacklight](#).” Blacklight is a privacy-inspection tool developed by The Markup, a nonprofit news publication focused on the impact of technology on society.¹² The tool allows users to input a website's URL into its search

¹ FED. TRADE COMM’N, [How Websites and Apps Collect and use Your Information](#), <https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information>.

² *Id.*

³ *See id.*

⁴ *See id.*

⁵ *See* Sam Morris, [I Scanned the Websites I Visit with Blacklight, and It’s Horrifying. Now What?](#), The Markup (Sept. 22, 2020), <https://themarkup.org/the-breakdown/2020/09/22/i-scanned-the-websites-i-visit-with-blacklight-and-its-horrifying-now-what>.

⁶ *Id.*

⁷ *See id.*

⁸ *Id.*

⁹ *See id.*

¹⁰ *See id.*

¹¹ *See id.*

¹² *See id.*

engine.¹³ Blacklight then provides a report detailing the number of trackers detected on the site and offers insights into the trackers' activities, such as whether the site permits keylogging.¹⁴

For the test, nine different websites were imputed into the Blacklight tool. These websites were categorized into three groups: retail websites (Amazon, Target, and Walmart), media websites (The New York Times, CNN, and FOX News), and health-related websites (Mayo Clinic, Cleveland Clinic, and WebMD).

III. Results: Online Tracking Across Different Websites¹⁵

	Websites	Ad Trackers Found on Site:	Third-Party Cookies Found:	Does website evade third-party cookie blockers?	Does website use session recording?	Does website capture keystrokes?	Does website use Facebook Pixel?	Does website use Google Analytics?
Retail	Amazon	0	0	No	No	No	No	No
	Target	9	2	Yes	No	No	No	No
	Walmart	13	9	No	No	No	Site tells Facebook of visit even if cookies are blocked	No
Media	New York Times	21	29	No	No	No	No	No
	CNN	52	97	No	No	No	No	No
	FOX News	70	127	Yes	No	No	No	No
Health	Mayo Clinic	1	2	No	No	No	No	No
	Cleveland Clinic	8	20	No	No	No	No	No
	WebMD	40	96	No	No	No	Site tells Facebook of visit	No

IV. Analyzing the Results

A. Retail Websites

In the context of retail websites, there is a notable difference in online tracking practices between Amazon, Target, and Walmart. This difference is primarily attributed to Amazon's online privacy strategy known as "Wall Guard."¹⁶ Amazon's Wall Guard serves as a barrier that inhibits third-party tracking on its site.¹⁷ Instead of relying on third-party trackers, Amazon tracks user behavior within its own digital ecosystem. Consequently, suppliers have the option to pay a premium for enhanced visibility and higher placement on the Amazon website. For instance, a manufacturer of bicycle tubes can opt to pay Amazon for an elevated advertising status. This ensures prominent product placement in search results, enhancing discoverability among

¹³ See *id.*

¹⁴ See *id.*

¹⁵ See [Blacklight](https://themarkup.org/blacklight), The Markup (Sept. 22, 2020), <https://themarkup.org/blacklight>.

¹⁶ Brian X. Chen and Daisuke Wakabayashi, [How You're Still Being Tracked on the Internet](https://www.nytimes.com/2022/04/06/technology/online-tracking-privacy.html), The New York Times (Apr. 6, 2022), <https://www.nytimes.com/2022/04/06/technology/online-tracking-privacy.html>.

¹⁷ See *id.*

shoppers. Amazon's ability to directly negotiate with marketers and suppliers for product placement on its site circumvents the need for third-party trackers. Furthermore, the presence of Amazon Prime, a subscription-based service, reduces Amazon's reliance on third-party trackers as a source of revenue.

In contrast, Walmart and Target, do not possess the same influence and market size as Amazon. Consequently, they permit other third-party marketers to track users on their platforms. These retailers track Walmart and Target website users to curate targeted advertisements. In return, Walmart and Target receive compensation from these third-party trackers.¹⁸ This distinction highlights the impact financial size has on the approach to online tracking. Amazon's strategic deployment of the Wall Guard and its subscription-based model allows it to reduce reliance on third-party trackers, while Walmart and Target, given their relative market positions, opt for an approach reliant on third-party tracking.

B. Media Websites

Regarding media websites, a significant contrast arises when examining the prevalence of online trackers on The New York Times, CNN, and FOX News. The distinguishing factor is The New York Times has a subscription-based model, which restricts access to paying subscribers only. This approach leads to a reduced reliance on third-party trackers as a primary revenue source. Consequently, the New York Times can afford to employ fewer external tracking mechanisms on its website.

In contrast, CNN and FOX News have an open-access approach, allowing any internet user to visit their websites without subscription requirements. As a result, third-party trackers become essential for financing the operations and content of CNN and FOX. Essentially, subscription-based services like The New York Times tend to minimize their dependence on third-party trackers as a primary source of revenue. Conversely, media outlets such as CNN and FOX News have developed a reliance on third-party tracking for their economic sustainability.

C. Health Websites

In the realm of health websites, a large discrepancy exists regarding online tracking for the websites of the Mayo Clinic, Cleveland Clinic, and WebMD. Notably, the Mayo Clinic and the Cleveland Clinic track website users far less than WebMD. This difference arises from the fundamental natures of the Mayo Clinic and Cleveland Clinic: primarily brick-and-mortar patient care institutions, providing hands-on healthcare services (e.g., doctors, nurses, and physicians). Consequently, most of their revenue is derived from in-person patient care, rendering them less dependent on third-party trackers to fund their online platforms.¹⁹

¹⁸ *See id.*

¹⁹ *See* Jeff Kiger, Mayo Clinic reports strong finances for 2023 so far with Q2 revenue of \$4.47 billion, Post Bulletin (Aug. 17, 2023), <https://www.postbulletin.com/business/mayo-clinic-reports-strong-finances-for-2023-so-far-with-q2-revenue-of-4-47-billion#:~:text=Under%20assets%2C%20Mayo%20Clinic%20reported,for%20this%20quarter%20in%202022.>

Conversely, WebMD operates solely as an online health information website. As a result, its revenue stream is exclusively tied to its website. Therefore, WebMD relies on advertisements and engages in extensive third-party tracking to sustain its operations. In summary, the Mayo Clinic and the Cleveland Clinic, as in-person patient care providers, engage in minimal online tracking, while WebMD, functioning solely as an online health information resource, heavily relies on third-party tracking due to its exclusive dependence on its website for revenue generation.

V. Conclusion

The Blacklight study underscores significant concerns that internet users should acknowledge when navigating various websites. Presently, the United States lacks comprehensive legislation addressing online tracking, leaving users without clear protections.²⁰ To address this gap, the United States should consider implementing laws like those in the European Union.²¹ Such regulations would mandate websites to afford users the right to opt-out of both cookies and ad tracking.²² The absence of such protective measures results in a continuous violation of Americans' privacy every time they access the internet. Establishing robust legal frameworks is imperative to safeguard user privacy in the digital landscape.

²⁰ See Harrison Jacobs, Is Momentum Shifting Toward a Ban on Behavioral Advertising?, The Markup (Feb. 3, 2022), <https://themarkup.org/the-breakdown/2022/02/03/is-momentum-shifting-toward-a-ban-on-behavioral-advertising>.

²¹ See *id.*

²² *Id.*