LOKKER
POWERING PRIVACY.

How The Trackers Stole Christmas 2022

Shoppers unknowingly lost their personal data through a variety of web tracking technologies this holiday season

ONLINE DATA PRIVACY REPORT

JANUARY 2023

US shoppers spent over $35 billion online shopping this holiday season.

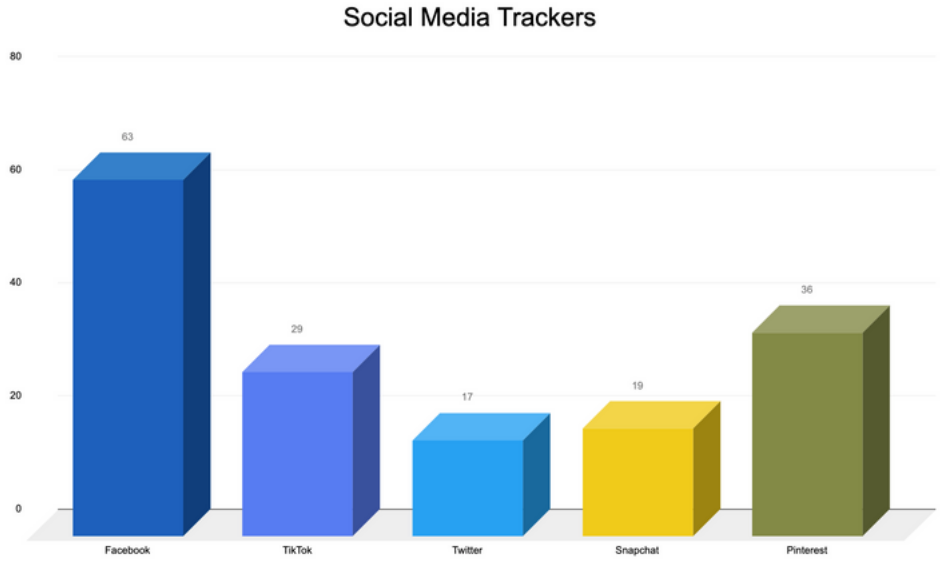
During the 2022 holiday season, Americans made a record amount of online purchases. While they were shopping, many of these e-commerce websites used trackers, pixels, and cookies to collect, analyze, share, sell, and resell our personal information. Shoppers inadvertently gave a lot of personal information to organizations they likely don't know. In order to determine how customer data was gathered, shared, and sold this holiday season, LOKKER examined the top 100 e-commerce websites in the US.

The 2022 holiday shopping season was unlike any other.

From Thanksgiving through Cyber Monday, US shoppers set a new sales record, spending slightly over $35 billion on online purchases. While 2022 saw record sales for online merchants, social media businesses and data brokers also went on a data-gathering binge, acquiring shoppers' personal information.

While Santa might know if you've been naughty or nice, the social media networks know even more!

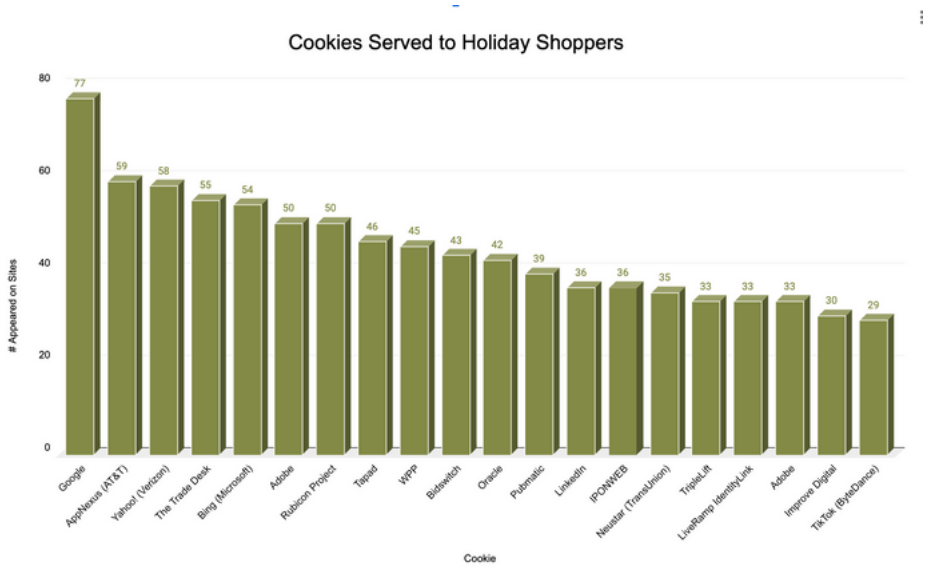
According to LOKKER'S research, Facebook tracked users on more than 60 of the most popular shopping websites, Pinterest on 35, and TikTok on 22. The final two social media platforms in the top 5, Twitter and Snapchat, are present on 18 and 19 of the top 100 websites. These platforms know which sites and pages we visited, what products we searched for, our locations, and so on. (This explains why you keep seeing pickleball advertisements in your feed.)



Just like Santa, shoppers got served a lot of cookies this year.

One of the most popular web tracking technologies, browser cookies, were present during most of our online shopping trips. Cookies are web apps that store data about how people use a website. Frequently, they are used for practical reasons like keeping track of the items added to a shopping cart as visitors browse other pages and products on a website. Advertising networks and data brokers may also use cookies to store a special ID code that can help identify and group our online activities into one profile. These codes may contain information about our searches, the articles and videos we watch, the health issues we research, and, yes, the holiday gifts we ultimately buy.

More than 3,000 cookies were served across the top 100 US shopping websites, according to the research, and as many as 134 cookies could be found on one website. Google's Doubleclick ad network had dropped the most cookies (discovered on 77 sites), which was followed closely by Microsoft (found on 59 sites), Verizon (found on 58), Experian (found on 46), and Oracle (on 42 of the top 100 websites).



The items that we shopped, the travel arrangements we made to visit friends and relatives, the sweaters, hats, and the Nutcracker tickets we bought were all under surveillance by various web trackers.

Each of these operates in the background of the most popular e-commerce websites, gathering data regarding the pages we view, the products we are interested in, our location, and additional websites we visit both before and after shopping.

The Usual Suspects Snatching Up Holiday Shoppers' Data

1. Google
2. Facebook
3. Microsoft
4. Verizon
5. Adobe
6. Experian
7. Oracle
8. Pinterest
9. Taboola
10. TransUnion

How can you protect your customers in 2023?

Companies in every sector (including marketers, IT specialists, and data protection executives) must be more alert about securing customer data in the new year as California, Colorado, Connecticut, Virginia, and Utah roll out new privacy legislation. Here are some suggestions on how to make 2023 secure for your online clients and conform to the new laws:

1. Inspect your website for 3rd party pixels, tags, and trackers and ensure you have business relationships in place with each
2. Use consent management software to clarify to your customers what data is being collected, by whom, and for what purpose
3. Check that pages collecting client form data do not contain risky third-party programs, and make sure they are configured correctly to not "overshare" data with your partners (such as session replay tools and tracking pixels).

Here's to a prosperous 2023 and creating a better and safer internet for everyone.