



July 2024

Tracking You By Mark Costlow

We are never alone on the Internet. Making a reservation or purchase late at night while the rest of the house is quiet may seem like an intimate transaction between two parties. But there is a crush of onlookers, hovering in the shadows just out of view, observing, scrutinizing, and recording your every movement.

That sounds like overwrought hyperbole but it is a common feeling when people realize how much of their online activity is being observed.

In our last issue, we introduced the **data brokers** and what they are collecting. We discussed who their customers are and **what they do with the data**. We mentioned one source of their location data, software libraries embedded in the apps we use. But there are other sources, and in this issue we'll talk about the big one: ad networks and exchanges.

Ad Automation

Most blog, news, or recipe sites you visit use a 3rd party ad network to provide ads. The web site you are visiting is only slightly involved in the ads you see. They don't create them, select them, or even approve them. All of that is outsourced to an **ad exchange**.

Displaying an ad on a web site is a surprisingly complicated and sophisticated operation. We will give an abbreviated explanation of the process below, and point you to two good companion sources which explain in more depth:

- **This 5½ minute video** from the Interactive Advertising Bureau gives a fairly complete overview of the process quickly and clearly.

- **This is a Real-Time Bidding overview from Alpha Quantum**, who develops software for this industry.

Note that since these are industry insiders, they don't emphasize some of the disturbing side-effects of the system. That will be our job.

A Blog Serves an Ad

When you visit a site (a "publisher") with ads on it, part of the page tells your browser to request an ad from the publisher's ad server. In most cases, the request is forwarded to a **Supply-Side Platform (SSP)**.

The SSP combines everything it knows about the situation:

- The publisher wanting to display an ad.
- The specific type of content you are accessing, including keywords (e.g. sports, finance, TV and movies).
- Data the SSP can find about **you** specifically from external data sources.
- The data your browser submitted in the request for an ad, possibly including your precise or general location.

The SSP submits this compiled data to an Ad Exchange, which is where things get more interesting. The exchange runs an **RTB (Real-Time Bid) auction** for your eyeballs. It submits all the information provided by the SSP to a host of other parties, primarily **Demand-Side Platforms (DSPs)**, which are aggregators of advertisement inventory from many advertisers. Also included may be other ad networks and other ad exchanges. The chief requirement for all of these players to participate in the auction is that they have to return their bid incredibly fast, in less than 1/10th of a second.

As depicted in the drawing from Wikipedia below, the SSP is on one side, managing requests from publishers to show ads. DSPs are on the other side, managing inventory of ads available for sale. The Ad Exchange is in the middle, executing the RTB, and obtaining an ad for your browser to display.

The benefit of this system for the advertisers is they can place their ads only where they will have the most impact. If they want to reach

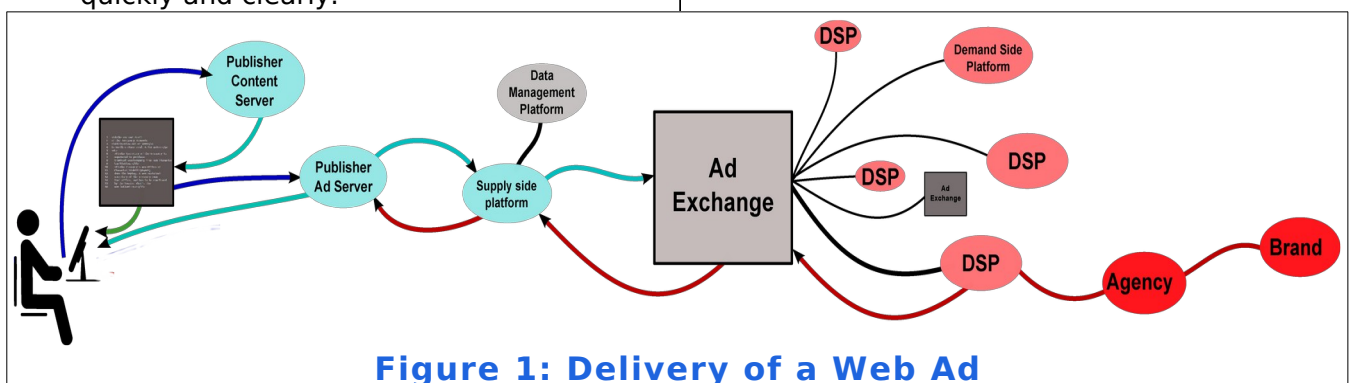


Figure 1: Delivery of a Web Ad

pet owners, new moms, or any other demographic or **psychographic** group, they can pinpoint them. There is little point advertizing medicare plans to children, or snow blowers to Las Cruces residents.

For the consumer, the benefit is the other side of the same coin - seeing only ads you might be interested in. If you're under 30, you probably don't want to care about arthritis meds, and if you're over 60 you may have little interest in a new dance club opening.

For ad agencies and DSPs, the RTB guarantees the highest price for their ad inventory.

Everybody wins, right?

The Hidden Cost

The unspoken but obvious "payment" in this arrangement is your data. Many people will have already done the mental calculation, "I'm giving up some of my data to this advertiser in exchange for using this web site, that's not so bad". The hidden cost is that you did not give up your data to one entity that you think you know. Rather, you gave it up to a whole room full of anonymous harvesters.

The problem is the auction. **All of the participants receive all of the data.** Maybe they all scrupulously discard the data after each auction, or maybe not. There are movements to create **ethical frameworks for the handling of user data in RTBs**, but they are not actual regulations or laws, just suggested practices. Most of these frameworks, such as **The IAB's OpenRTB** are focused around making RTBs compliant with the European **GDPR** regulations. That will be helpful for Europeans, but does not necessarily help American consumers.

Minimizing the Payment

There's no way to opt out of this arrangement and still participate in the digital ecosystem. A recent visit to news site **cnn.com** caused my computer to connect to 125 other domains to display one page. Some of these are innocuous, elements required to serve the content. But *125 is a lot*. That's over 100 entities who were given some information about me. A quick random check into 6 of the domains that were unfamiliar (not clearly part of CNN, Time Warner, or other well-known companies like Yahoo, Google, and Amazon) revealed that 5 of them were indeed advertizing/data facilitators with descriptions such as, "a company that helps brands use customer data and other licensed data to improve customer interactions".

Visiting the site after turning on the popular ad blocker **uBlock Origin** prevented 26% of the requests and reduced the domain count from 125 to 28. It didn't cut them off completely, but it certainly slowed the flow (and sped up the page display in the bargain).

The relatively new **Do Not Track** feature of most web browsers can help by telling those who will listen that you don't want your clicks tracked across the web. The **EFF** has information about **Do Not Track and follow-on efforts**, as well as a site that will show you just **how trackable your web browser is**. They have discovered that the combination of your computer type, screen size, installed system fonts, and other innocuous information can be combined to "fingerprint" your specific browser and follow you even when cookies are not allowed.

Some argue that using ad blockers deprives web publishers of the revenue they need to provide the content you want cheaply or for free. This may be true, but it is also true that **the advertising + data broker cabal has betrayed the trust of consumers and you owe them nothing**.

This conflict is currently playing out on Youtube, as they have stepped up efforts to disallow ad blockers. They have tried to make it impossible to use the site with an ad blocker enabled. The easiest way to get rid of the ads there is to pay for Youtube Premium. **Some of your subscription money is shared with the creators**, rather than creators relying on you to view ads around their content. I have decided that is the best way forward for me and I pay the subscription fee. If I decide the Youtube content is not worth the fee, I can stop. For now, I get access to the content I want, the creators get compensation, and fewer data brokers get my data.

Youtube is just one site though. Subscribing to every site you want to visit is clearly not reasonable. But neither is a web choked with invasive tracking-enabled advertisements. Using an ad blocker and directly supporting creators you admire through subscription fees as on Youtube or **Medium**, or even more directly through sites like **Patreon**, seems like an imperfect middle ground. But until (or unless) the privacy pendulum swings back in our direction, that may be the best we can do.

So, install ad blockers, enable the "Do Not Track" setting in your web browser, click "NO" every time your browser asks to share your location, disallow location services for most of the apps on your phone, and don't feel bad about any of it.

Southwest Cyberport - swcp.com

*New Mexico's Expert Internet Service
Provider since 1994*

505-232-7992 | Support: help@swcp.com

5021 Indian School NE, Ste. 600,

Albuquerque, NM 87110

Click on bold blue text in browser for links.